

# Quantum repeaters and quantum key distribution: analysis of secret key rates

Silvestre Abruzzo<sup>1</sup>, Sylvia Bratzik<sup>1</sup>, Nadja K Bernardes<sup>2</sup>,  
Hermann Kampermann<sup>1</sup>, Peter van Loock<sup>2,3</sup> and Dagmar Bruß<sup>1</sup>

<sup>1</sup> Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf,  
Universitätsstr. 1, 40225 Düsseldorf, Germany

<sup>2</sup> Optical Quantum Information Theory Group, Max Planck Institute for the Science  
of Light, Günther-Scharowsky-Str. 1/Bau 24, 91058 Erlangen, Germany, and  
Institute of Theoretical Physics I, Universität Erlangen-Nürnberg, Staudtstr. 7/B2,  
91058 Erlangen, Germany

<sup>3</sup> Institute of Physics, Johannes-Gutenberg Universität Mainz, Staudingerweg 7,  
55128 Mainz, Germany

E-mail: [abruzzo@thphy.uni-duesseldorf.de](mailto:abruzzo@thphy.uni-duesseldorf.de),  
[bratzik@thphy.uni-duesseldorf.de](mailto:bratzik@thphy.uni-duesseldorf.de), [nadja.bernardes@mpl.mpg.de](mailto:nadja.bernardes@mpl.mpg.de)

**Abstract.** We analyse various prominent quantum repeater protocols in the context of long-distance quantum key distribution. These protocols are the original quantum repeater proposal by Briegel *et al*, the so-called hybrid quantum repeater using optical coherent states dispersively interacting with atomic spin qubits, and the DLCZ-type repeater using atomic ensembles together with linear optics and, in its most recent extension, heralded qubit amplifiers. For our analysis, we investigate the most important experimental parameters of every repeater component and find their minimally required values for obtaining a non-zero secret key. Additionally, we examine in detail the impact of device imperfections on the final secret key rate and on the optimal number of rounds of distillation when the entangled states are purified right after their initial distribution.

PACS numbers: 03.67.Hk, 03.67.Dd, 03.67.-a, 03.67.Bg, 42.50.Ex

**Contents**

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>General framework</b>	<b>3</b>
2.1	Quantum repeater . . . . .	3
2.1.1	The protocol . . . . .	3
2.1.2	Building blocks of the quantum repeater and their imperfections .	4
2.1.3	Generation rate of long-distance entangled pairs . . . . .	7
2.2	Quantum key distribution (QKD) . . . . .	9
2.2.1	The quantum bit error rate (QBER) . . . . .	10
2.2.2	The secret key rate . . . . .	11
2.3	Methods . . . . .	12
<b>3</b>	<b>The original quantum repeater</b>	<b>12</b>
3.1	The set-up . . . . .	12
3.2	Performance in the presence of imperfections . . . . .	14
<b>4</b>	<b>The hybrid quantum repeater</b>	<b>19</b>
4.1	The set-up . . . . .	19
4.2	Performance in the presence of imperfections . . . . .	21
<b>5</b>	<b>Quantum repeaters based on atomic ensembles</b>	<b>25</b>
5.1	The set-up . . . . .	26
5.2	Performance in the presence of imperfections . . . . .	30
<b>6</b>	<b>Conclusions</b>	<b>34</b>

**1. Introduction**

Quantum communication is one of the most exciting and well developed areas of quantum information. Quantum key distribution (QKD) is a sub-field, where two parties, usually called Alice and Bob, want to establish a secret key. For this purpose, typically, they perform some quantum operations on two-level systems, the qubits, which, for instance, can be realized by using polarized photons. In this paper, we assume that Alice and Bob trust completely their measurement apparatus. To be more realistic, it is possible to relax this assumption and to consider device-independent quantum key distribution (DI-QKD) [1, 2, 3, 4, 5]. An analysis of the performance of long-distance DI-QKD can also be done using those methods that we will develop in this paper. However, here the focus is on standard QKD over large distances.

Photons naturally have a long decoherence time and hence could be transmitted over long distances. Nevertheless, recent experiments show that QKD so far is limited to about 150 km [6], due to losses in the optical-fibre channel. Hence, the concept of

quantum relays and repeaters was developed [7, 8, 9, 10, 11]. These aim at entangling qubits over long distances by means of entanglement swapping and entanglement distillation. There exist various proposals for an experimental implementation, such as those based upon atomic ensembles and single-rail entanglement [12], the hybrid quantum repeater [13], the ion-trap quantum repeater [14], repeaters based on deterministic Rydberg gates [15, 16], and repeaters based on nitrogen-vacancy (NV) centres in diamond [17].

In this paper, we analyse the performance of quantum repeaters within a QKD set-up, calculating secret key rates as a function of the relevant experimental parameters. Previous investigations on long-distance QKD either consider quantum relays [9, 11, 18], which only employ entanglement swapping without using quantum memories or entanglement distillation, or, like the works in [19, 20], they exclusively refer to the original Duan-Lukin-Cirac-Zoller quantum repeater [12]. Here, our aim is to quantify the influence of characteristic experimental parameters on the secret key rate for three different repeater schemes, namely the original quantum repeater protocol [7], the hybrid quantum repeater [13], and a recent variation of the DLCZ-repeater [21]. In order to reduce the complexity of every full repeater protocol, we always allow entanglement distillation to take place only directly after the initial entanglement distribution. The influence of distillation during later stages of the repeater, as well as the comparison between different distillation protocols, will be studied elsewhere [22].

This manuscript is organized as follows: In section 2 we present a description of the relevant parameters of a quantum repeater, as well as the main tools for analysing its performance for QKD. This section should also provide a general framework for analysing other existing quantum repeater protocols, and for studying the performance and the potential of new protocols. Sections 3, 4, and 5 investigate long-distance QKD protocols for three different quantum repeater schemes; these sections can be read independently. Section 3 is devoted to the original proposal for a quantum repeater [7], section 4 analyses the hybrid quantum repeater [13], and finally, in section 5, we investigate quantum repeaters with atomic ensembles [12]. The conclusion will be given in section 6, and more details on the calculations will be presented in the appendix.

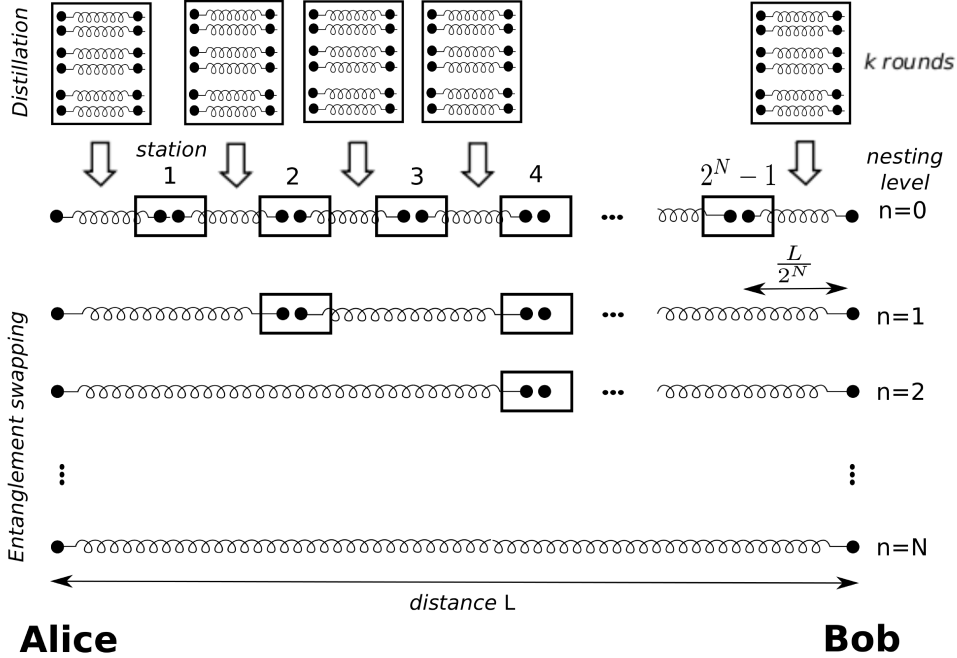
## 2. General framework

### 2.1. Quantum repeater

The purpose of this section is to provide a general framework that describes formally the theoretical analysis of a quantum repeater.

*2.1.1. The protocol* Let  $L$  be the distance between the two parties Alice and Bob who wish to share an entangled state. A quantum repeater consists of a chain of  $2^N$  segments of fundamental length  $L_0 := L/2^N$  and  $2^N - 1$  repeater stations which are placed at the intersection points between two segments (see figure 1). Each repeater

station is equipped with quantum memories and local quantum processors to perform entanglement swapping and, in general, also entanglement distillation. In consecutive *nesting levels*, the distances over which the entangled states are shared will be doubled. The parameter  $N$  is the *maximal nesting level*.



**Figure 1.** Scheme of a generic quantum repeater protocol. We adopt the nested protocol proposed in [7]. The distance between Alice and Bob is  $L$ , which is divided in  $2^N$  segments, each having the length  $L_0 := L/2^N$ . The parameter  $n$  describes the different nesting levels, and the value  $N$  represents the maximum nesting level. In this paper, we consider quantum repeaters where distillation is performed exclusively before the first entanglement swapping step. The number of distillation rounds is denoted by  $k$ .

The protocol starts by creating entangled states in all segments, i.e., between two quantum memories over distance  $L_0$ . After that, if necessary, entanglement distillation is performed. This distillation is a probabilistic process which requires sufficiently many initial pairs shared over distance  $L_0$ . As a next step, entanglement swapping is performed at the corresponding repeater stations in order to connect two adjacent entangled pairs and thus gradually extend the entanglement. In those protocols where entanglement swapping is a probabilistic process, the whole quantum repeater protocol is performed in a recursive way as shown in figure 1. Whenever the swapping is deterministic (i.e., it never fails), then all swappings can be executed simultaneously, provided that no further probabilistic entanglement distillation steps are to be incorporated at some intermediate nesting levels for enhancing the fidelities. Recall that in the present work, we do not include such intermediate distillations.

*2.1.2. Building blocks of the quantum repeater and their imperfections* In this section, we describe the imperfections that can be present in a quantum repeater.

*Quantum channel* Let us consider photons (in form of single- or multi-photon pulses) travelling through optical fibres. In this case, losses scale exponentially with the length  $\ell$ , i.e., the transmittivity is given by [8]

$$\eta_t(\ell) := 10^{-\frac{\alpha_{att}\ell}{10}}, \quad (1)$$

where  $\alpha_{att}$  is the attenuation coefficient given in dB/km. The lowest attenuation is achieved in the telecom wavelength range around 1550 nm and it corresponds to  $\alpha_{att} = 0.17$  dB/km. This attenuation will also be used throughout the paper. Note that other types of quantum channels, such as free space, can be treated in an equivalent way (see e.g. [23]). Further note that besides losses we do not explicitly include channel errors that would cause decoherence of the initially prepared entangled states. Instead, the entire effect of the quantum channel is absorbed into what we consider the initial state, i.e., the state which is shared between two neighbouring repeater stations over distance  $L_0$  (see below). The amplitude damping that occurs in these elementary segments typically has a significant impact on the final pair generation and secret key rates, either directly through a decreasing number of detectable photons at the receiving stations or indirectly through a decrease of the entanglement fidelity (like for the hybrid quantum repeater which uses multi-photon pulses).

*Source of entanglement* The purpose of a source is to create entanglement between quantum memories over distance  $L_0$ . An ideal source produces maximally entangled Bell states (see below) on demand. In practice, however, the created state may not be maximally entangled and may be produced in a probabilistic way. We denote by  $\rho_0$  a state shared between two quantum memories over the elementary distance  $L_0$  and by  $P_0$  the total probability to generate and distribute this state. This probability would contain any finite local state-preparation probabilities before the distribution, the effect of channel losses, and the success probabilities of other processes, such as the conditioning on a desired initial state  $\rho_0$  after the state distribution over  $L_0$ .

For improving the scaling over the total distance  $L$  from exponential to sub-exponential, it is necessary to have a heralded creation and storage of  $\rho_0$ . How this heralding is implemented depends on the particular protocol and it usually involves a form of post-processing, e.g. conditioning the state on a specific pattern of detector clicks. This can also be a finite postselection window of quadrature values in homodyne detection. However, in the present work, the measurements employed in all protocols considered here are either photon-number measurements or Pauli measurements on memory qubits.

*Detectors* We will consider photon-number resolving detectors (PNRD) which can be described by a positive-operator valued measure (POVM) [24] with elements

$$\Pi^{(n)} := \eta_d^n \sum_{m=0}^{\infty} \binom{n+m}{n} (1 - \eta_d)^m |n+m\rangle \langle n+m|. \quad (2)$$

Here,  $\Pi^{(n)}$  is the element of the POVM related to the detection of  $n$  photons,  $\eta_d$  is the efficiency of the detector, and  $|n + m\rangle$  is a state of  $(n + m)$ -photons. In the POVM above, we have neglected dark counts; we have proven analytically for those protocols considered in this paper that realistic dark counts of the order of  $10^{-5}$  are negligible. Note that we consider PNRD throughout this work; of course, the whole analysis could also be extended to threshold detectors.

*Gates* Imperfections of gates also depend on the particular quantum repeater protocol. In our analysis, we will characterize them using only one parameter which describes a particular type of error. The gate quality will be denoted by  $p_G$  (see (19) and (24)). Other types of imperfections can be modelled in an analogous way.

*Quantum memories* Quantum memories are a crucial part of a quantum repeater. Here, we will not explicitly study the role of decoherence in form of some additional memory error model such as memory dephasing. Such decoherence effects have been studied independently of QKD in [25, 26], but also in the context of QKD in [26]. However, here we do include a memory quantum efficiency represented by the parameter  $\eta_m$ , whenever it is appropriate. This is the probability that a photon is released when a reading signal is applied to the quantum memory, or, more generally, the probability that an initial qubit state is still intact after write-in, storage, and read-out.

*Entanglement distillation* As mentioned before, throughout this work we only consider distillation at the beginning of each repeater protocol. Entanglement distillation is a probabilistic process requiring local multi-qubit gates and classical communication. In this paper, we consider the protocol by Deutsch *et al* [27]<sup>†</sup>. This protocol performs especially well when there are different types of errors (e.g. bit flips and phase flips). However, depending on the particular form of the initial state and on the particular quantum repeater protocol, other distillation schemes may perform better (see [22] for a detailed discussion). The Deutsch *et al* protocol starts with  $2^k$  pairs and after  $k$  rounds, it produces one entangled pair with higher fidelity than at the beginning. Every round requires two CNOTs, each performed on two qubits at the same repeater station, and projective measurements with post-selection.

Distillation has two main sources of errors: imperfect quantum gates which no longer permit to achieve the ideal fidelity, as well as imperfections of the quantum memories and the detectors, decreasing the success probability. We denote the success probability in the  $i$ -th distillation round by  $P_D[i]$ .

*Entanglement swapping* In order to extend the initial distances of the shared entanglement, entanglement swapping can be achieved through a Bell measurement

<sup>†</sup> For the quantum repeater with atomic ensembles (section 5), we do not consider any additional distillation on two or more initial memory pairs.

performed at the corresponding stations between two adjacent segments. Such a Bell measurement can be, in principle, realized using a CNOT gate and suitable projection measurements on the corresponding quantum memories [28]. An alternative implementation of the Bell measurement uses photons released from the quantum memories and linear optics [29]. This last technique is probabilistic, but typically much less demanding from an experimental point of view.

We should emphasize that the final single-qubit rotation depending on the result of the Bell measurement, as generally needed to complete the entanglement swapping step, is not necessary when the final state is used for QKD applications. In fact, it simply corresponds to suitable bit flip operations on the outcomes of the QKD measurements, i.e., the effect of that single-qubit rotation can be included into the classical post-processing.

Imperfections of entanglement swapping are characterized by the imperfections of the gates (which introduce noise and therefore a decrease in fidelity) and by the imperfections of the measurement process, caused by imperfect quantum memories and imperfect detectors. We denote the probability that entanglement swapping is successful in the  $n$ -th nesting level by  $P_{\text{ES}}^{(n)}$ .

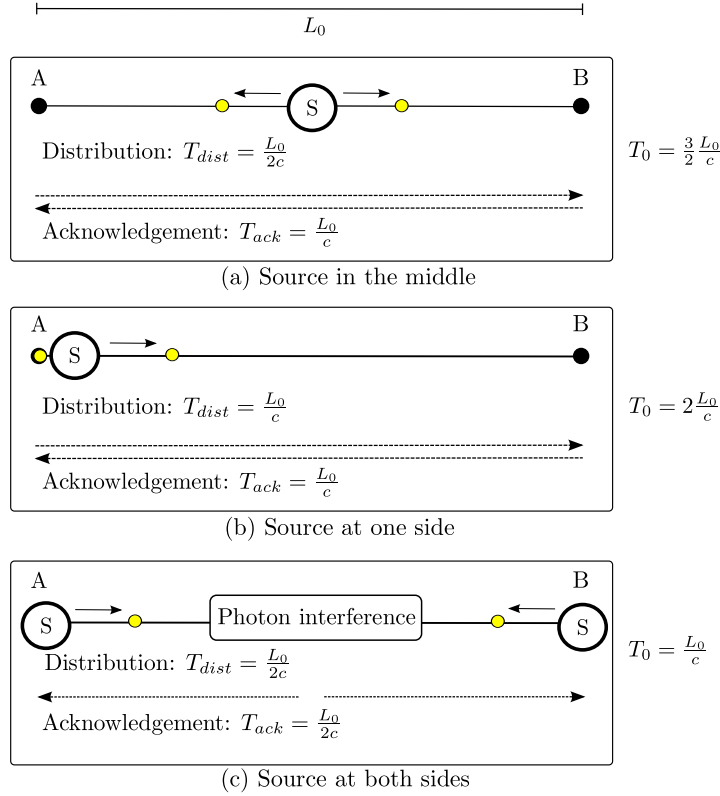
*2.1.3. Generation rate of long-distance entangled pairs* In order to evaluate the performance of a quantum repeater protocol it is necessary to assess how many entangled pairs across distance  $L$  can be generated per second.

A relevant unit of time is the *fundamental time* needed to communicate the successful distribution of an elementary entangled pair over distance  $L_0$ , which is given by:

$$T_0 := \frac{\beta L_0}{c}, \quad (3)$$

where  $c = 2 \cdot 10^5$  km/s is the speed of light in the fibre channel (see e.g. [30]) and  $\beta$  is a factor depending on the type of entanglement distribution. Note that here we have neglected the additional local times needed for preparing and manipulating the physical systems at each repeater station. Figure 2 shows three different possibilities how to model the initial entanglement distribution. The fundamental time  $T_0$  consists of the time to distribute the photonic signals,  $T_{\text{dist}}$ , and the time of acknowledgment,  $T_{\text{ack}}$ , which all together can be different for the three cases shown.

Throughout the paper, we denote the average number of final entangled pairs produced in the repeater per second by  $R_{\text{REP}}$ . We emphasize that regarding any figures and plots, for each protocol, we are interested in the consumption of time rather than spatial memories. Thus, if one wants to compare different set-ups for the same number of spatial memories, one has to rescale the rates such that the number of memories becomes equal. For example, in order to compare a protocol without distillation with another one with  $k$  rounds of distillation, one has to divide the rates for the case with distillation by  $2^k$  (as we need two initial pairs to obtain one distilled pair in every round).



**Figure 2.** The fundamental time for different models of entanglement generation and distribution. The source (S) that produces the initial entangled states is either placed in the middle (a), at one side (b), or at both sides (c). In the latter case, photons are emitted from a source and interfere in the middle (see [31, 32]).

In the literature, two different upper bounds on the entanglement generation rate  $R_{\text{REP}}$  are known. In the case of deterministic entanglement swapping ( $P_{ES}^{(n)} = 1$ ) we have [33]

$$R_{\text{REP}}^{\text{det}} := (T_0 Z_N(P_{L_0}[i]))^{-1}, \quad (4)$$

with  $P_{L_0}[i]$  being a recursive probability depending on the rounds of distillation  $i$  as follows [33]

$$P_{L_0}[i = 0] = P_0, \quad (5)$$

$$P_{L_0}[i > 0] = \frac{P_D[i]}{Z_1(P_{L_0}[i-1])}. \quad (6)$$

We remind the reader that  $P_D[i]$  is the success probability in the  $i$ -th distillation round. Here,

$$Z_N(P_0) := \sum_{j=1}^{2^N} \binom{2^N}{j} \frac{(-1)^{j+1}}{1 - (1 - P_0)^j} \quad (7)$$

is the average number of attempts to connect  $2^N$  pairs, each generated with probability  $P_0$ .



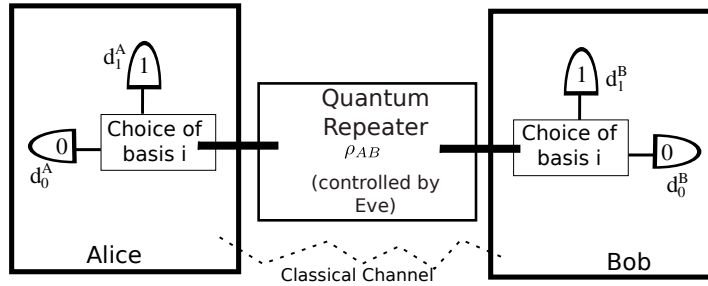
In the case of probabilistic entanglement swapping, we define:

$$R_{\text{REP}}^{\text{prob}} := \frac{1}{T_0} \left( \frac{2}{3} \right)^{N+k} P_0 P_{ES}^{(1)} P_{ES}^{(2)} \dots P_{ES}^{(N)} \prod_{i=1}^k P_D[i]. \quad (8)$$

Note that the quantities above should be interpreted as limiting upper bounds (see Appendix A) on the repetition rates, derived from the minimal times needed for communicating the quantum and classical signals. For this minimal time duration, we consider explicitly only those communication times for initially generating entanglement, but not those for entanglement swapping and entanglement distillation.

## 2.2. Quantum key distribution (QKD)

*The QKD protocol* In figure 3 a general quantum key distribution set-up is shown. For long-distance QKD, Alice and Bob will generate entangled pairs using the quantum repeater protocol. For the security analysis of the whole repeater-based QKD scheme, we assume that a potential eavesdropper (Eve) has complete control of the repeater stations, the quantum channels connecting them, and the classical channels used for communicating the measurement outcomes for entanglement swapping and distillation (see figure 3). The QKD protocol itself starts with Alice and Bob performing measurements on their shared, long-distance entangled pairs (see figure 3). For this purpose, they would both independently choose a certain measurement from a given set of measurement settings. The next step is the classical post-processing and for this an authenticated channel is necessary. First, Alice and Bob discard those measurement outcomes where their choice of the setting did not coincide (sifting), thus obtaining a raw key associated with a *raw key rate*. They proceed by comparing publicly a small subset of outcomes (parameter estimation). From this subset, they can estimate the *quantum bit error rate* (QBER), which corresponds to the fraction of uncorrelated bits. If the QBER is below a certain threshold, they apply an error correction protocol and privacy amplification in order to shrink the eavesdropper's information about the secret key (for more details, see e.g. [34]).



**Figure 3.** Scheme of quantum key distribution. The state  $\rho_{AB}$  is produced using a quantum repeater. Alice and Bob locally rotate this state in a measurement basis and then they perform the measurement. The detectors are denoted by  $d_0^A, d_1^A, d_0^B, d_1^B$  and to each detector click a classical outcome is assigned.

Various QKD protocols exist in the literature. Besides the original QKD protocol by Bennett and Brassard from 1984, the so-called BB84-protocol [35], the first QKD protocol based upon entanglement was the Ekert protocol [1]. Shortly thereafter the relation of the Ekert protocol to the BB84-protocol was found [36]. Another protocol which can also be applied in entanglement-based QKD is the six-state protocol [37, 38].

*2.2.1. The quantum bit error rate (QBER)* In order to evaluate the performance of a QKD protocol, it is necessary to determine the quantum bit error rate. This is the fraction of discordant outcomes when Alice and Bob compare a small amount of outcomes taken from a specified measurement basis. This measurement can be modelled by means of four detectors (two on Alice's side and two on Bob's side, see figure 3) where to each detector click a classical binary outcome is assigned. Particular care is necessary when multi-photon states are measured [39]. In the following, we give the definition of the QBER for the case of photon-number-resolving detectors and we refer to [20] for the definition in the case of threshold detectors. The probability that a particular detection pattern occurs is given by

$$P_{jklm}^{(i)} := \text{tr} \left( \Pi_{d_0^A}^{(j)} \Pi_{d_1^A}^{(k)} \Pi_{d_0^B}^{(l)} \Pi_{d_1^B}^{(m)} \rho_{AB}^{(i)} \right), \quad (9)$$

where the POVM  $\Pi^{(n)}$  has been defined in (2) with a subscript denoting the detectors given in figure 3. The superscript  $i$  refers to the measurement basis and  $\rho_{AB}^{(i)}$  represents the state  $\rho_{AB}$  rotated in the basis  $i$ .

A valid QKD measurement event happens when one detector on Alice's side and one on Bob's side click. The probability of this event is given by [20]

$$P_{\text{click}}^{(i)} := P_{1010}^{(i)} + P_{0101}^{(i)} + P_{0110}^{(i)} + P_{1001}^{(i)}. \quad (10)$$

The probability that two outcomes do not coincide is given by [20]

$$P_{\text{err}}^{(i)} := P_{0110}^{(i)} + P_{1001}^{(i)}. \quad (11)$$

Thus, the fraction of discordant bits, i.e., the quantum bit error rate for measurement basis  $i$  is [20]

$$e_i := \frac{P_{\text{err}}^{(i)}}{P_{\text{click}}^{(i)}}. \quad (12)$$

For the case that  $\rho_{AB}$  is a two-qubit state, we find that the QBER does not depend on the efficiency of the detectors, as  $P_{\text{click}}^{(i)} = \eta_d^2$  and  $P_{\text{err}}^{(i)} \propto \eta_d^2$ .

If we assume a genuine two-qubit system<sup>‡</sup> like in the original quantum repeater proposal (see section 3) or the hybrid quantum repeater (see section 4), without loss of generality<sup>§</sup>, the entangled state  $\rho_{AB}$  can be considered diagonal in the Bell-basis, i.e.,

<sup>‡</sup> Note that the states of the DLCZ-type quantum repeaters (see section 5) are only effectively two-qubit states, when higher-order excitations of the atom-light entangled states [12], or those of the states created through parametric down conversion [21], are neglected.

<sup>§</sup> As proven in [40, 41], it is possible to apply an appropriate local twirling operation that transforms an arbitrary two-qubit state into a Bell diagonal state, while the security of the protocol is not compromised.

$\rho_{AB} = A|\phi^+\rangle\langle\phi^+| + B|\phi^-\rangle\langle\phi^-| + C|\psi^+\rangle\langle\psi^+| + D|\psi^-\rangle\langle\psi^-|$ , with the probabilities  $A, B, C, D$ ,  $A + B + C + D = 1$ , and with the dual-rail¶ encoded Bell states\*\*  $|\phi^\pm\rangle = (|1010\rangle \pm |0101\rangle)/\sqrt{2}$  and  $|\psi^\pm\rangle = (|1001\rangle \pm |0110\rangle)/\sqrt{2}$  (we shall use the notation  $|\phi^\pm\rangle$  and  $|\psi^\pm\rangle$  for the Bell basis in any type of encoding throughout the paper). Then the QBER along the directions  $X$ ,  $Y$ , and  $Z$  corresponds to [6]

$$e_X := B + D, \quad e_Z := C + D, \quad e_Y := B + C. \quad (13)$$

Throughout the whole paper  $X$ ,  $Y$  and  $Z$  denote the three Pauli operators acting on the restricted Hilbert space of qubits.

*2.2.2. The secret key rate* The figure of merit representing the performance of quantum key distribution is the *secret key rate*  $R_{\text{QKD}}$  which is the product of the *raw key rate*  $R_{\text{raw}}$  (see above) and the *secret fraction*  $r_\infty$ . Throughout this paper, we will use asymptotic secret key rates. The secret fraction represents the fraction of secure bits that may be extracted from the raw key. Formally, we have

$$R_{\text{QKD}} := R_{\text{raw}} r_\infty = R_{\text{REP}} P_{\text{click}} R_{\text{sift}} r_\infty, \quad (14)$$

where the sifting rate  $R_{\text{sift}}$  is the fraction of measurements performed in the same basis by Alice and Bob; e.g. for the original BB84-protocol one has  $R_{\text{sift}} = \frac{1}{2}$ . We point out that both  $R_{\text{REP}}$  and  $r_\infty$  are functions of the explicit repeater protocol and the involved experimental parameters, as we will discuss in detail later. When maximizing the overall secret key rate  $R_{\text{QKD}}$ , there will be a trade-off between  $R_{\text{REP}}$  and  $r_\infty$ , as the secret key fraction  $r_\infty$  is an increasing function of the final fidelity, while the repeater rate  $R_{\text{REP}}$  typically decreases with increasing final fidelity.

The secret fraction represents the fraction of secure bits over the total number of measured bits. We adopt the *composable security definition* discussed in [42, 43]. Here, composable means that the secret key can be used in successive tasks without compromising its security.

In the present work, we consider only two QKD protocols, namely the BB84-protocol and the six-state protocol, for which collective and coherent attacks are equivalent [40, 41] in the limit of a large number of exchanged signals. The unique parameter entering the formula of the secret fraction is the quantum bit error rate (QBER).

In the BB84-protocol only two of the three Pauli matrices are measured. We adopt the asymmetric protocol where the measurement operators are chosen with different probabilities [44], because this leads to higher key rates. We call  $X$  the basis used for extracting a key, i.e., the basis that will be chosen with a probability of almost one in the measurement process, while  $Z$  is the basis used for the estimation of the QBER.

¶ In this paper, by *dual-rail representation* we mean that a single photon can be in a superposition of two optical modes, thus representing a single qubit. By *single-rail representation* we mean that a qubit is implemented using only one single optical mode. See [24] for additional details.

\*\*The ket  $|abcd\rangle$  is a vector in a Hilbert space of four modes and the values of  $a$ ,  $b$ ,  $c$  and  $d$  represent the number of excitations in the Fock basis.

Thus, in the asymptotic limit, we have  $R_{\text{sift}} = 1$ . The formula for the secret fraction is [6]

$$r_{\infty}^{\text{BB84}} := 1 - h(e_Z) - h(e_X), \quad (15)$$

with  $h(p) := -p \log_2 p - (1-p) \log_2 (1-p)$  being the binary entropy. This formula is an achievable upper bound on the secret fraction.

In the six-state protocol we use all three Pauli matrices. We call  $X$  the basis used for extracting a key, which will be chosen with a probability of almost one, and both  $Y$  and  $Z$  are the bases used for parameter estimation. In this case, the formula for the secret fraction is given by [6, 34]<sup>††</sup>

$$r_{\infty}^{6S} := 1 - e_Z h\left(\frac{1 + (e_X - e_Y)/e_Z}{2}\right) - (1 - e_Z) h\left(\frac{1 - (e_X + e_Y + e_Z)/2}{1 - e_Z}\right) - h(e_Z). \quad (16)$$

### 2.3. Methods

The secret key rate represents the central figure of merit for our investigations. We study the BB84-protocol, because it is most easily implementable and can also be used for protocols, where  $\rho_{AB}$  is not a two-qubit state, with help of the squashing model [39]. Throughout the paper, we also report on results of the six-state protocol if applicable. In the previous sections, we have described all the relevant analytical formulas needed to calculate the secret key rate. We have performed the explicit calculations using the software Mathematica [45]. We did not use any approximations except for the quantum repeater based on atomic ensembles where we truncate the states and cut off the higher excitations at some maximal number (see section 5 for the details). For the optimizations, we have used the numerical functions provided by Mathematica.

## 3. The original quantum repeater

In this section, we consider a general class of quantum repeaters in the spirit of the original proposal by Briegel *et al* [7]. We will analyse the requirements for the experimental parameters such that the quantum repeater is useful in conjunction with QKD.

### 3.1. The set-up

The set-up that we consider in this section is applicable whenever two-qubit entanglement is distributed by using qubits encoded into single photons. This is the case, for instance, for quantum repeaters based on ion traps or Rydberg-blockade gates. We emphasize that we do not aim to capture all peculiarities of a specific set-up. Instead, our intention is to present a fairly general analysis that can give an idea of the order of magnitude, which has to be achieved for the relevant experimental parameters.

<sup>††</sup>Note that the formula for the six-state protocol is independent of the choice of basis, when we assume the state of Alice and Bob  $\rho_{AB}$  to be Bell diagonal. Then the secret fraction reduces to  $r_{\infty}^{6S} = 1 - S(\rho_E)$  with  $S(\rho)$  the von Neumann entropy and  $\rho_E$  is the eavesdropper's state.

*Elementary entanglement creation* The probability that two adjacent repeater stations (separated by distance  $L_0$ ) share an entangled pair is given by

$$P_0 := \eta_t(L_0), \quad (17)$$

where  $\eta_t(\ell)$ , as defined in (1), is the probability that a photon is not absorbed during the channel transmission. In a specific protocol,  $P_0$  may contain an additional multiplicative factor such as the probability that entanglement is heralded or also a source efficiency. We assume that the state created over distance  $L_0$  is a depolarized state of fidelity  $F_0$  with respect to  $|\phi^+\rangle$ , i.e.,

$$\rho_0 := F_0 |\phi^+\rangle \langle \phi^+| + \frac{1-F_0}{3} (|\psi^+\rangle \langle \psi^+| + |\psi^-\rangle \langle \psi^-| + |\phi^-\rangle \langle \phi^-|). \quad (18)$$

The fidelity  $F_0$  contains the noise due to an imperfect preparation and the noise in the quantum channel. We have chosen a depolarized state, because this corresponds to a generic noise model and, moreover, any two-qubit mixed quantum state can be brought into this form using local twirling operations [46].

*Imperfect gates* For the local qubit operations, such as the CNOT gates, we use a generic gate model with depolarizing noise, as considered in [7]. Thus, we assume that a noisy gate  $O_{BC}$  acting upon two qubits  $B$  and  $C$  can be modelled by

$$O_{BC}\rho_{BC} = p_G O_{BC}^{\text{ideal}} \rho_{BC} + \frac{1-p_G}{4} \mathbb{1}_{BC}, \quad (19)$$

where  $O_{BC}^{\text{ideal}}$  is the ideal gate operation and  $p_G$  describes the gate quality. Note that, in general, the noisy gates realized in an experiment do not necessarily have this form, however, such a noise model is useful for having an indication as to how good the corresponding gates must be. Other noise models could be analogously incorporated into our analysis. Further, we assume that one-qubit gates are perfect.

*Entanglement distillation* We consider entanglement distillation only before the first entanglement swapping steps, right after the initial pair distributions over  $L_0$ . We employ the Deutsch *et al* protocol [27] which indeed has some advantages, as shown in the analysis of [22]. In Appendix B.2, we review this protocol and we also present the corresponding formulas in the presence of imperfections. We point out that when starting with two copies of depolarized states, the distillation protocol will generate an output state which is no longer a depolarized state, but instead a generic Bell diagonal state. Distillation requires two-qubit gates, which we describe using (19). Different from the original Briegel *et al* scheme [7], we do not perform an additional twirling operation in order to have once again a depolarized state. The reason is that this depolarization would require additional experimental effort and, even more importantly, we have seen from our simulations that this step would produce lower secret key rates.

*Entanglement swapping* The entanglement connections are performed through entanglement swapping by implementing a (noisy) Bell measurement on the photons stored in two local quantum memories. We consider a Bell measurement that is deterministic in the ideal case. It is implemented using a two-qubit gate with gate quality  $p_G$  (see (19)). Analogous to the case of distillation, starting with two depolarized states, at the end of the noisy Bell measurement, we will obtain generic Bell diagonal states. Also in this case, it turns out that a successive depolarization decreases the secret key rate and this step is therefore not performed in our scheme.

### 3.2. Performance in the presence of imperfections

The secret key rate (14) represents our central object of study, as it characterizes the performance of a QKD protocol. It can be written explicitly as a function of the relevant parameters,

$$R_{\text{QKD}}^{\text{O}} = R_{\text{REP}}(L_0, F_0, N, p_G, \eta_d, k) P_{\text{click}}(\eta_d) R_{\text{sift}} r_{\infty}(F_0, p_G, N, k), \quad (20)$$

where  $R_{\text{REP}}$  is given by (4) when  $\eta_d = 1$  (because then  $P_{\text{ES}} = 1$ ) or by (8) if  $\eta_d < 1$ <sup>††</sup>. The probability that the QKD measurement is successful is given by  $P_{\text{click}} = \eta_d^2$  and the secret fraction  $r_{\infty}$  is given by either (15) or (16), depending on the type of QKD protocol. For the asymmetric BB84-protocol, we have  $R_{\text{sift}} = 1$  (see section 2.2). The superscript O refers to the original quantum repeater proposal as considered in this section. In order to have a non-zero secret key rate, it is then necessary that the repeater rate, the probability for a valid QKD measurement event, and the secret fraction are each non-zero too. As typically  $R_{\text{REP}} > 0$ ,  $R_{\text{sift}} > 0$  and  $P_{\text{click}} > 0$ , for  $R_{\text{QKD}} > 0$ , it is sufficient to have a non-zero secret fraction,  $r_{\infty} > 0$ . The value of the secret fraction does not depend on the distance, and therefore some properties of this protocol are distance-invariant.

*Minimally required parameters* In this paragraph, we will discuss the minimal requirements that are necessary to be able to extract a secret key, i.e., we will specify the parameter region where the secret fraction is non-zero. From the discussion in the previous paragraph, we know that this region does not depend on the total distance, but only on the initial fidelity  $F_0$ , the gate quality  $p_G$ , the number of segments  $2^N$ , and the maximal number of distillation rounds  $k$ . Moreover, note that even if the secret fraction is not zero, the total secret key rate can be very low (see below).

<sup>††</sup>The supposed link between the effect of imperfect detectors and the determinism of the entanglement swapping here assumes the following. Any incomplete detection patterns that occur in the Bell measurements due to imperfect detectors are considered as inconclusive results and will be discarded. Conversely, with perfect detectors, we assume that we always have complete patterns and thus the Bell state discrimination becomes complete too. Note that this kind of reasoning directly applies to Bell measurements in dual-rail encoding, where the conclusive output patterns always have the same fixed total number for every Bell state (namely two photons leading to two-fold detection events), and so any loss of photons will result in patterns considered inconclusive. In single-rail encoding, the situation is more complicated and patterns considered conclusive may be the result of an imperfect detection.

**Table 1.** Minimal initial fidelity  $F_0$  ( $p_G$  is fixed to one) for extracting a secret key with maximal nesting level  $N$  and number of distillation rounds  $k$  for the BB84- and six-state protocols.

N \ k	0		1		2		3	
	BB84	6S	BB84	6S	BB84	6S	BB84	6S
0	0.835	0.810	0.733	0.728	0.671	0.669	0.620	0.614
1	0.912	0.898	0.821	0.818	0.742	0.740	0.669	0.664
2	0.955	0.947	0.885	0.884	0.801	0.800	0.713	0.709
3	0.977	0.973	0.929	0.928	0.849	0.848	0.752	0.749
4	0.988	0.987	0.957	0.957	0.887	0.887	0.788	0.785
5	0.994	0.993	0.975	0.975	0.917	0.917	0.819	0.818
6	0.997	0.997	0.985	0.985	0.939	0.939	0.847	0.846
7	0.999	0.998	0.992	0.992	0.956	0.956	0.872	0.870

**Table 2.** Minimal  $p_G$  ( $F_0$  is fixed to one) for extracting a secret key with maximal nesting level  $N$  and number of distillation rounds  $k$  for the BB84- and six-state protocols.

N \ k	0		1		2		3	
	BB84	6S	BB84	6S	BB84	6S	BB84	6S
0	-	-	0.800	0.773	0.869	0.860	0.891	0.884
1	0.780	0.748	0.922	0.910	0.942	0.937	0.947	0.942
2	0.920	0.908	0.965	0.960	0.973	0.970	0.974	0.972
3	0.965	0.959	0.984	0.981	0.987	0.986	0.987	0.986
4	0.984	0.981	0.992	0.991	0.994	0.993	0.994	0.993
5	0.992	0.991	0.996	0.995	0.997	0.997	0.997	0.997
6	0.996	0.995	0.998	0.998	0.999	0.998	0.999	0.998
7	0.998	0.998	0.999	0.999	0.999	0.999	0.999	0.999

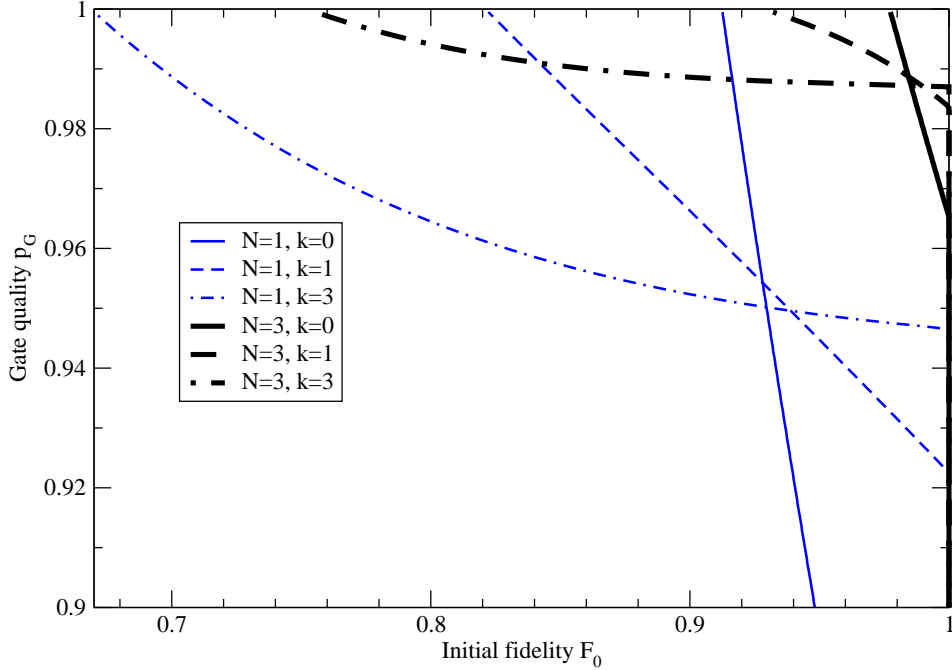
For calculating the minimally required parameters, we start with the initial state in (18), we distil it  $k$  times (see the formulas in Appendix B.2), and then we swap the distilled state  $2^N - 1$  times (see the formulas in Appendix B.1). At the end, a generic Bell diagonal state is obtained. Using (13) one can then calculate the QBER, which is sufficient to calculate the secret fraction.

Table 1 and table 2 show the minimally required values for  $F_0$  and  $p_G$  for different maximal nesting levels  $N$  (i.e., different numbers of segments  $2^N$ ) and different numbers of rounds of distillation  $k$ . Throughout these tables, we can see that for the six-state protocol, the minimal fidelity and the minimal gate quality  $p_G$  are lower than for the BB84-protocol. Our results confirm the intuition that the larger the number of distillation rounds, the smaller the affordable initial fidelity can be.

In figure 4, the lines represent the values of the minimal initial fidelity and the minimal gate quality for a specific  $N$  that allow for extracting a secret key. As shown



in figure 4, any lower initial fidelity requires a correspondingly higher gate quality and vice versa.

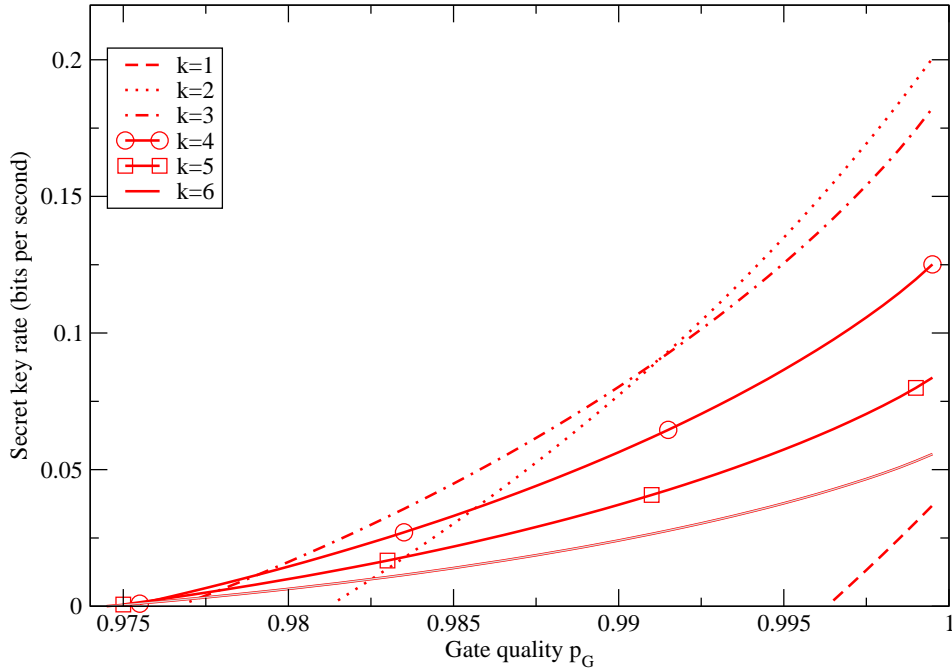


**Figure 4.** Original quantum repeater and the BB84-protocol: Minimal initial fidelity  $F_0$  and minimal gate quality  $p_G$  permitting to extract a secret key for various maximal nesting levels  $N$  and numbers of distillation rounds  $k$ .

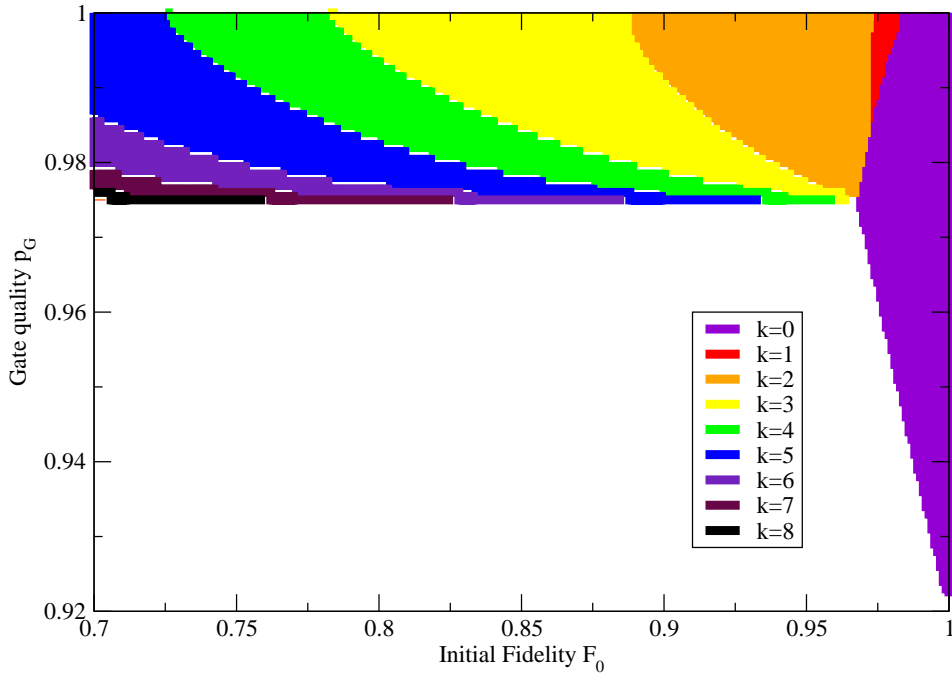
*The secret key rate* In this section, we will analyse the influence of the imperfections on the secret key rate, see (20).

In figure 5 we illustrate the effect of gate imperfections on the secret key rate for different numbers of rounds of distillation and for fixed values of distance, initial fidelity, and maximal number of nesting levels. Throughout this whole section, we use  $\beta = 2$  in (3) for the fundamental time, which corresponds to the case where a source is placed at one side of an elementary segment (see figure 2). The optimal number of distillation rounds decreases as  $p_G$  increases. We see from the figure that  $k = 2$  is optimal when  $p_G = 1$ . This is due to the fact that from  $k = 1$  to  $k = 2$ , the raw key rate decreases by 40%, but the secret fraction increases by 850%. However, from  $k = 2$  to  $k = 3$ , the raw key rate decreases once again by 40%, but now the secret fraction increases only by 141%. In this case, the net gain is smaller than 1 and therefore three rounds of distillation do not help to increase the secret key rate compared to the case of two rounds. In other words, what is lost in terms of success probability when having three probabilistic distillation rounds is not added to the secret fraction. For a decreasing  $p_G$ , more rounds of distillation become optimal. The reason is that when the gates become worse, additional rounds of distillation permit to increase the secret key rate sufficiently much to compensate the decrease of  $R_{\text{REP}}$ .



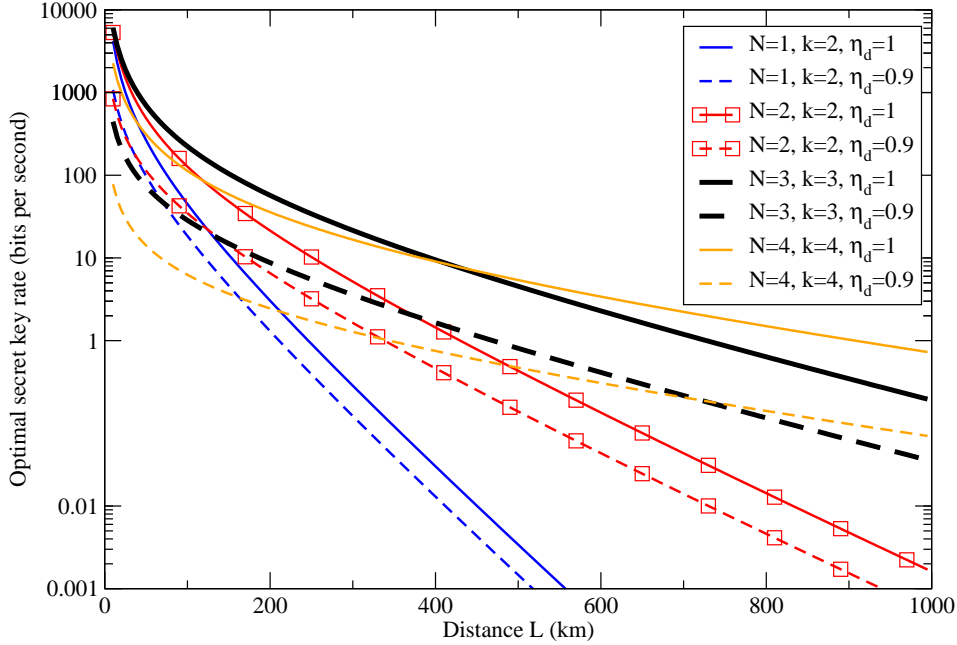


**Figure 5.** Original quantum repeater and the BB84-protocol: Secret key rate (20) versus gate imperfections  $p_G$  for different rounds of distillation  $k$ . The case  $k = 0$  leads to a vanishing secret key rate. (Parameters:  $F_0 = 0.9$ ,  $N = 2$ ,  $L = 600$  km)



**Figure 6.** Original quantum repeater and the BB84-protocol: Number of distillation rounds  $k$  that maximizes the secret key rate as a function of gate quality  $p_G$  and initial fidelity  $F_0$ . In the white area, it is no longer possible to extract a secret key. (Parameters:  $N = 2$ ,  $L = 600$  km)

In figure 6 we show the optimal number of rounds of distillation  $k$  as a function of the imperfections of the gates and the initial fidelity. It turns out that when the experimental parameters are good enough, then distillation is not necessary at all.



**Figure 7.** Original quantum repeater and the BB84-protocol: Optimal secret key rate (20) versus distance for different nesting levels, with and without perfect detectors. For each maximal nesting level  $N$ , we have chosen the optimal number of distillation rounds  $k$ . A nesting level  $N \geq 5$  no longer permits to obtain a non-zero secret key rate. (Parameters:  $F_0 = 0.9$  and  $p_g = 0.995$ .)

Let us now investigate the secret key rate (20) as a function of the distance  $L$  between Alice and Bob. In figure 7 the secret key rate for the optimal number of distillation rounds versus the distance for various nesting levels is shown, for a fixed initial fidelity and gate quality. These curves should be interpreted as upper bounds; when additional imperfections are included, the secret key rate will further decrease. We see that for a distance of more than 400 km, the value  $N = 4$  (which corresponds to 16 segments) is optimal. Note that with the initial fidelity and gate quality assumed here, it is no longer possible to extract a secret key for  $N = 5$ .

In many implementations, detectors are far from being perfect. The general expression of the raw key rate including detector efficiencies  $\eta_d$  becomes

$$R_{\text{raw}} = \frac{1}{T_0} R_{\text{sift}} \left( \frac{2}{3} \right)^{N+k} \eta_d^{2(k+N+1)} P_0 \prod_{i=1}^k P_D[i], \quad (21)$$

using (14) with the repeater rate  $R_{\text{REP}}$  given by (8). The term  $\eta_d^{2k}$  arises from the two-fold detections for the distillation, and similarly,  $\eta_d^{2N}$  comes from the entanglement swapping and  $\eta_d^2$  from the QKD measurements.

In figure 7 we observe that even if detectors are imperfect, it is advantageous to do the same number of rounds of distillation as for the perfect case. This is due to the fact

that the initial fidelity is so low that even with a lower success probability, the gain in the secret fraction produces a net gain greater than 1.

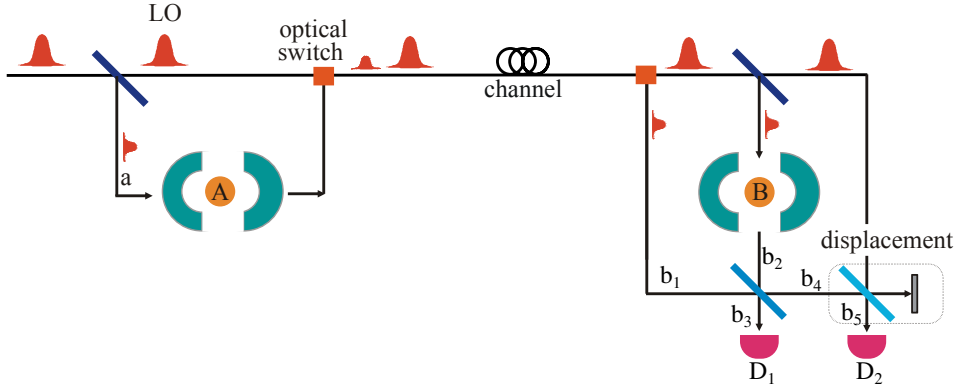
For realistic detectors, the dark count probability is much smaller than their efficiency. We show in Appendix B that, provided that the dark count probability is smaller than  $10^{-5}$ , dark counts can be neglected. This indeed applies to most modern detectors [47].

## 4. The hybrid quantum repeater

In this section, we will investigate the so-called hybrid quantum repeater (HQR) introduced by van Loock *et al* [13] and Ladd *et al* [48]. In this scheme, the resulting entangled pairs are discrete atomic qubits, but the probe system (also called *qubus*) that mediates the two-qubit entangling interaction is an optical mode in a coherent state. The scheme does not only employ atoms and light at the same time, but it also uses both discrete and continuous quantum variables; hence the name hybrid. The entangled pair is conditionally prepared by suitably measuring the qubus after it has interacted with two atomic qubits located in the two spatially separated cavities at two neighboring repeater stations. Below we shall consider a HQR where the detection is based on an unambiguous state discrimination (USD) scheme [49, 50]. In this case, arbitrarily high fidelities can be achieved at the expense of low probabilities of success.

### 4.1. The set-up

*Elementary entanglement creation* Entanglement is shared between two electronic spins (such as  $\Lambda$  systems effectively acting as two-level systems) in two distant cavities (separated by  $L_0$ ). The entanglement distribution occurs through the interaction of the coherent-state pulse with both atomic systems. The coherent-state pulse and the cavity are in resonance, but they are detuned from the transition between the ground state and the excited state of the two-level system. This interaction can then be described by the Jaynes-Cummings interaction Hamiltonian in the limit of large detuning,  $H_{int} = \hbar\chi Z a^\dagger a$ , where  $\chi$  is the light-atom coupling strength,  $a$  ( $a^\dagger$ ) is the annihilation (creation) operator of the electromagnetic field mode, and  $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$  is the  $Z$  operator for a two-level atom (throughout this section,  $|0\rangle$  and  $|1\rangle$  refer to the two  $Z$  Pauli eigenstates of the effective two-level matter system and not to the optical vacuum and one-photon Fock states). After the interaction of the qubus in state  $|\alpha\rangle$  with the first atomic state, which is initially prepared in a superposition, the output state is  $U_{int} [|\alpha\rangle (|0\rangle + |1\rangle)/\sqrt{2}] = (|\alpha e^{-i\theta/2}\rangle |0\rangle + |\alpha e^{i\theta/2}\rangle |1\rangle)/\sqrt{2}$ , with  $\theta = 2\chi t$  an effective light-matter interaction time inside the cavity. The qubus probe pulse is then sent through the lossy fibre channel and interacts with the second atomic qubit also prepared in a superposition. Here we consider the protocol of [50], where linear optical elements and photon detectors are used for the unambiguous discrimination of the phase-rotated coherent states. Different from [50], however, we use imperfect photon-number-resolving



**Figure 8.** Schematic diagram for the entanglement generation by means of a USD measurement following [50]. The two quantum memories  $A$  and  $B$  are separated by a distance  $L_0$ . The part on the left side (an intermediate Alice) prepares a pulse in a coherent state  $|\alpha\rangle_a$  (the subscript refers to the corresponding spatial mode). This pulse first interacts with her qubit  $A$  and is then sent to the right side together with the local oscillator pulse (LO). The part on the right side (an intermediate Bob) receives the state  $|\sqrt{\eta_t}\alpha\rangle_{b_1}$  and produces from the LO through beam splitting a second probe pulse  $|\sqrt{\eta_t}\alpha\rangle_{b_2}$  which interacts with his qubit  $B$ . He further applies a 50:50 beam splitter to the pulses in modes  $b_1$  and  $b_2$ , and a displacement  $D(-\sqrt{2\eta_t}\alpha \cos \theta/2) = e^{-\sqrt{2\eta_t}\alpha \cos \theta/2(a^\dagger - a)}$  to the pulse in mode  $b_4$ . The entangled state is conditionally generated depending on the results of detectors  $D_1$  and  $D_2$ . The fibre attenuation  $\eta_t(L_0)$  has been defined in (1).

detectors (PNRD), as described by (2), instead of threshold detectors. By performing such a USD measurement on the probe state, as illustrated in figure 8, the following entangled state can be conditionally prepared,

$$\rho_0 := F_0 |\phi^+\rangle \langle \phi^+| + (1 - F_0) |\phi^-\rangle \langle \phi^-|, \quad (22)$$

where  $F_0 = [1 + e^{-2(1+\eta_t(1-2\eta_d))\alpha^2 \sin^2(\theta/2)}]/2$  (see Appendix C.1) for  $\alpha$  real,  $\eta_t(L_0)$  is the channel transmission given in (1), and  $\eta_d$  is the detection efficiency (see section 2.1.2). Note that the form of this state is different from the state considered in section 3. It is a mixture of only two Bell states, since the two other (bit flipped) Bell states are filtered out through the USD measurement. The remaining mixedness is due to a phase flip induced by the coupling of the qubus mode with the lossy fibre environment. The optimal probability of success to generate an entangled pair in state  $\rho_0$  can be found as

$$P_0 = 1 - (2F_0 - 1)^{\frac{\eta_t \eta_d}{1 + \eta_t(1 - 2\eta_d)}}, \quad (23)$$

which generalizes the formula for the quantum mechanically optimal USD with perfect detectors, as given in [49], to the case of imperfect, photon-number-resolving detectors. The derivation is given in Appendix C.1\*.

\* One may also measure the qubus using homodyne detection [13]. However, for this scheme, final fidelities would be limited to  $F_0 < 0.8$  for  $L_0 = 10$  km [13], whereas by using unambiguous state discrimination, we can tune the parameters for any distance  $L_0$ , such that the fidelity  $F_0$  can be chosen freely and, in particular, made arbitrarily close to unity at the expense of the success probability dropping close to zero [49].

*Entanglement swapping* A two-qubit gate is essential to perform entanglement swapping and entanglement distillation. In the HQR a controlled-Z (CZ) gate operation can be achieved by using dispersive interactions of another coherent-state probe with the two input qubits of the gate. This is similar to the initial entanglement distribution, but this time without any final measurement on the qubus [51]. Controlled rotations and uncontrolled displacements of the qubus are the essence of this scheme. The controlled rotations are realized through the same dispersive interaction as explained above. In an ideal scheme, after a sequence of controlled rotations and displacements on the qubus, the qubus mode will automatically disentangle from the two qubits and the only effect will be a sign flip on the  $|11\rangle$  component of the input two-qubit state (up to single-qubit rotations), corresponding to a CZ gate operation. Thus, this gate implementation can be characterized as measurement-free and deterministic. Using this gate, one can then perform a fully deterministic Bell measurement (i.e., one is able to distinguish between all four Bell states), and consequently, the swapping occurs deterministically (i.e.,  $P_{ES} \equiv 1$ ).

In a more realistic approach, local losses will cause errors in these gates. Following [52], after dissipation, we may consider the more general, noisy two-qubit operation  $O_{BC}$  acting upon qubits  $B$  and  $C$ ,

$$O_{BC}\rho_{BC} = O_{BC}^{ideal} (p_c^2(x)\rho_{BC} + p_c(x)(1 - p_c(x))(Z^B \rho_{BC} Z^B + Z^C \rho_{BC} Z^C) + (1 - p_c(x))^2 Z^B Z^C \rho_{BC} Z^C Z^B), \quad (24)$$

where

$$p_c(x) := \frac{1 + e^{-x/2}}{2} \quad (25)$$

is the probability for each qubit to not suffer a  $Z$  error, and  $x := \pi \frac{1-p_G^2}{\sqrt{p_G}(1+p_G)}$ ; here  $p_G$  is the local transmission parameter that incorporates photon losses in the local gates. The explicit formulas for entanglement swapping including imperfect two-qubit gates are given in Appendix C.2.

*Entanglement distillation* For the distillation, the same two-qubit operation as described above in (24) can be used. It is then interesting to notice that if we start with a state given in (22), after one round of imperfect distillation, the resulting state is a generic Bell diagonal state. The effect of gate errors in the distillation step is given in Appendix C.3<sup>†</sup>.

#### 4.2. Performance in the presence of imperfections

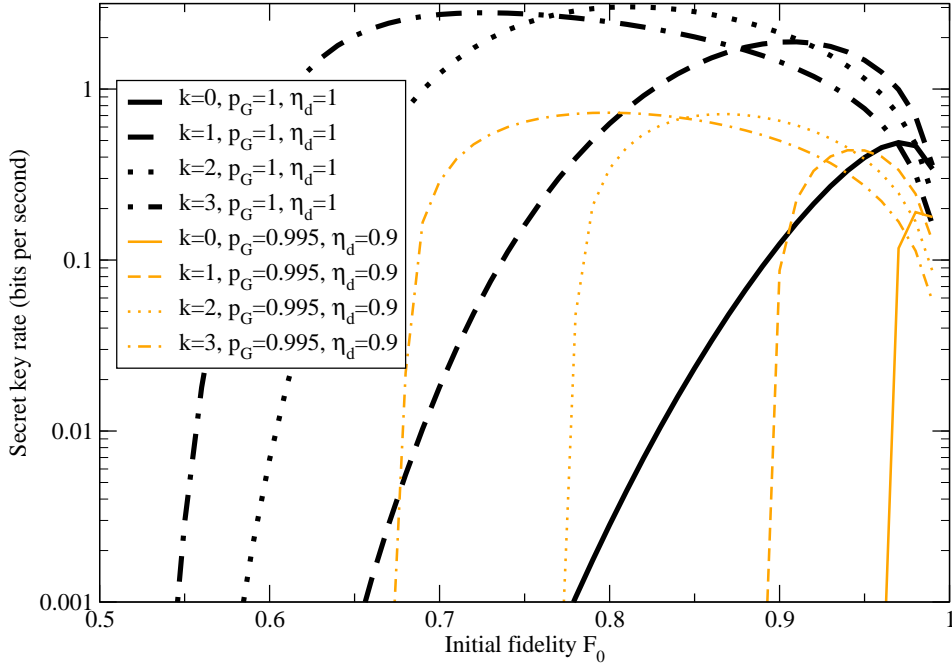
In the following, we will only consider the BB84-protocol, because it is experimentally less demanding and also, because we found in our simulations that the six-state protocol produces almost the same secret key rates, due to the symmetry of the state in (22).

<sup>†</sup> Note that we assume perfect qubit measurements for the distillation and the swapping, but imperfect two-qubit gates. Losses from the detectors can be absorbed into losses of the gates.

The secret key rate per second for the hybrid quantum repeater can be written as a function of the relevant parameters:

$$R_{\text{QKD}}^{\text{H}} = R_{\text{REP}}^{\text{det}}(L_0, F_0, p_G, \eta_d, N, k) R_{\text{sift}} r_{\infty}^{\text{BB84}}(L_0, F_0, p_G, N, k), \quad (26)$$

where  $R_{\text{REP}}^{\text{det}}$  is the repeater pair-creation rate for deterministic swapping (4) described in section 2.1.3 and  $r_{\infty}^{\text{BB84}}$  is the secret fraction for the BB84-protocol (15). For the asymmetric BB84-protocol, we have  $R_{\text{sift}} = 1$  (see section 2.2). The superscript H stands for hybrid quantum repeater. Note that the fundamental time is  $T_0 = \frac{2L_0}{c}$ , as the qubus is sent from Alice to Bob and then classical communication in the other direction is used (see section 2.1.3 and figure 2). Further notice that the final projective qubit measurements which are necessary for the QKD protocol are assumed to be perfect. Thus, the secret key rate presented here represents an upper bound and, depending on the particular set-up adopted for these measurements, it should be multiplied by the square of the detector efficiency.



**Figure 9.** Hybrid quantum repeater with perfect quantum operations ( $p_G = 1$ ) and perfect detectors ( $\eta_d = 1$ ) (black lines) compared to imperfect quantum operations ( $p_G = 0.995$ ) and imperfect detectors ( $\eta_d = 0.9$ ) (orange lines): Secret key rate per second (26) as a function of the initial fidelity for  $2^3$  segments ( $N = 3$ ) and various rounds of distillation  $k$ . The distance between Alice and Bob is 600 km.

*The secret key rate* Figure 9 shows the secret key rate for  $2^3$  segments ( $N = 3$ ) for various rounds of distillation. We see from the figure that for the hybrid quantum repeater the secret key rate is not a monotonic function of the initial fidelity. The reason is that increasing  $F_0$  decreases  $P_0$  (see (23)) and vice versa. We find that the optimal initial fidelity, i.e., the fidelity where the secret key rate is maximal, increases as

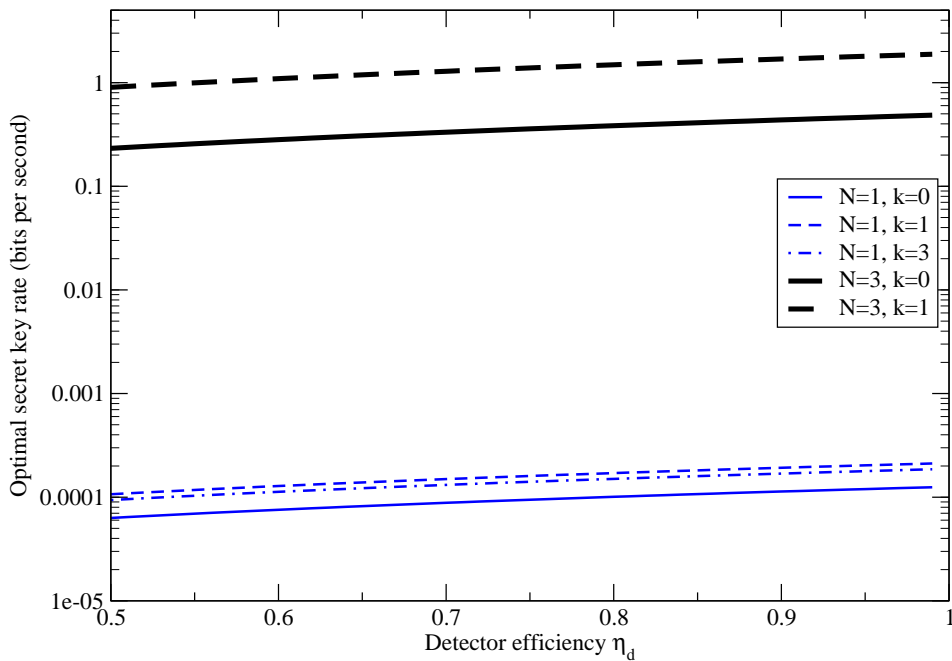
**Table 3.** Hybrid quantum repeater without imperfections ( $p_G = 1$  and  $\eta_d = 1$ ): Initial fidelity  $F_0$  that maximizes the secret key rate in (26) for a given number  $2^N$  of segments and  $k$  rounds of distillation.

N \ k	k			
	0	1	2	3
1	0.898	0.836	0.765	0.705
2	0.946	0.876	0.788	0.715
3	0.972	0.907	0.812	0.726
4	0.986	0.931	0.834	0.741

the maximal number of segments increases (see table 3). On the other hand, examining the optimal initial fidelity as a function of the distance, it turns out that it is almost constant for  $L > 100$  km. Thus, for such distances, it is neither useful nor necessary to produce higher fidelities, because these would not permit to increase the secret key rate.

We also observe that the maximum of the initial fidelity is quite broad for small  $N$ , and gets narrower as  $N$  increases. If we now consider perfect gates and perfect detectors, we see that by fixing a certain secret key rate, we can reach this value with lower initial fidelities by performing distillation. Furthermore, by distilling the initial entanglement, we can even exceed the optimal secret key rate without distillation by one order of magnitude. However, note that distillation for  $k$  rounds requires  $2^k$  memories at each side. If we then assume that we choose the protocol with no distillation and perform it in parallel  $2^k$  times, i.e., we use the same amount of memories as for the scheme including distillation, the secret key rate without distillation (as shown in figure 9) should be multiplied by  $2^k$ . As a result, the total secret key rate can then be even higher than that obtained with distillation.

Let us now assess the impact of the gate and detector imperfections on the secret key rate (orange lines) in figure 9. We notice that  $p_G$  has a large impact even if it is only changed by a small amount, like here from  $p_G = 1$  to  $p_G = 0.995$ ; the secret key rates drop by one order of magnitude. Imperfect detectors are employed in the creation of entanglement. As we see in figure 10, imperfect detectors do not affect the secret key rate significantly. As for  $N = 3$  and  $k = 0$ , improving the detector efficiency from 0.5 to 1 leads to a doubling of the secret key rate. We conclude that for the hybrid quantum repeater, the final secret key rates are much more sensitive to the presence of gate errors than to inefficiencies of the detectors. However, recall that in our analysis, we only take into account detector imperfections that occur during the initial USD-based entanglement distribution. Any measurements on the memory qubits performed in the local circuits for swapping and distillation are assumed to be perfect, whereas the corresponding two-qubit gates for swapping and distillation are modeled as imperfect quantum operations.

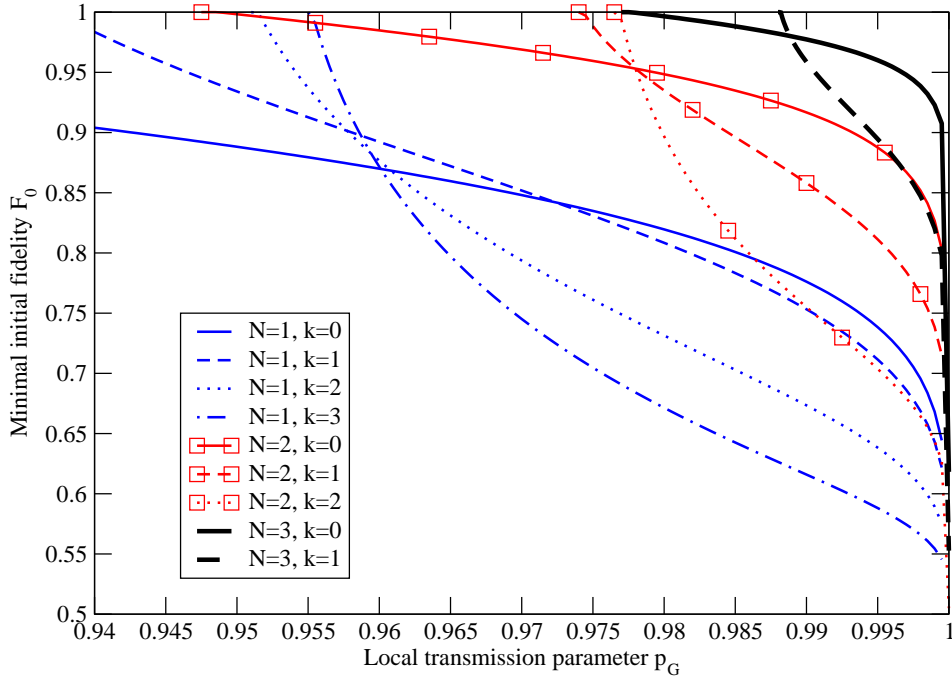


**Figure 10.** Hybrid quantum repeater with perfect gates ( $p_G = 1$ ): The optimal secret key rate (26) for the BB84-protocol in terms of the detector efficiency  $\eta_d$  for the distance  $L = 600$  km with various numbers of segments  $2^N$  and rounds of distillation  $k$ .

*Minimally required parameters* As we have seen in the previous section, it is also worth finding the minimal parameters for  $F_0$  and  $p_G$ , for which we can extract a secret key. Figure 11 shows the minimal initial fidelity required for extracting a secret key as a function of the local transmission probability  $p_G$ , which was introduced in section 4.1. We obtain also the minimal values of the local transmission probability  $p_{G,N}^{\min}$  without distillation (solid lines in figure 11). If  $p_G < p_{G,N}^{\min}$ , then it is no longer possible to extract a secret key. As shown in figure 11, these minimal values (for which the minimal initial fidelity becomes  $F_0 = 1$ , without distillation) are  $p_{G,1}^{\min} = 0.853$  (not shown in the plot),  $p_{G,2}^{\min} = 0.948$ ,  $p_{G,3}^{\min} = 0.977$ , and  $p_{G,4}^{\min} = 0.989$  (not shown in the plot). When including distillation, we can extend the regime of non-zero secret key rate to smaller initial fidelities at the cost of better local transmission probabilities. So there is a trade-off: if we can produce almost perfect Bell pairs, that is initial states with high fidelities  $F_0$ , we can afford larger gate errors. Conversely, if high-quality gates are available, we may operate the repeater with initial states having a lower fidelity. Note that these results and figure 11 do not depend on the length of each segment in the quantum repeater, but only on the number of segments.

In figure 12 we plotted the optimal secret key rate for a fixed local transmission probability  $p_G$  and detector efficiency  $\eta_d$  in terms of the total distance  $L$ . We varied the number of segments  $2^N$  and the number of distillation rounds  $k$ . We observe that a high value of  $k$  is not always advantageous: There exists for every  $N$  an optimal  $k$ , for which we obtain the highest key rate. We see, for example, that for  $N = 1$ , the optimal





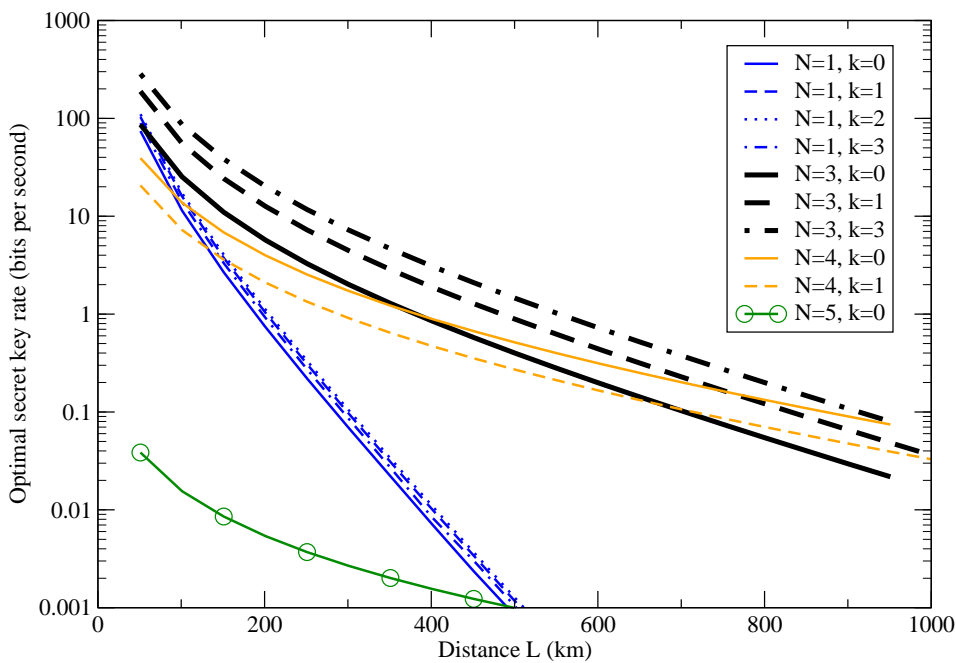
**Figure 11.** Hybrid quantum repeater with distillation and imperfections: Minimal initial fidelity as a function of the local transmission probability for various maximal numbers of segments  $2^N$  and rounds of distillation  $k$ . If the initial fidelity is smaller than the minimal initial fidelity, then it is no longer possible to extract a secret key. The lines with  $k = 0$  correspond to entanglement swapping without distillation.

choice is  $k = 2$ , whereas for  $N = 3$ , the optimal  $k$  is 3. One can also see that there are distances, where it is advantageous to double the number of segments if one wants to avoid distillation, as, for example, for  $N = 3$  and  $N = 4$  at a distance of around 750 km.

## 5. Quantum repeaters based on atomic ensembles

The probably most influential proposal for a practical realization of quantum repeaters was made in [12] and it is known as the Duan-Lukin-Cirac-Zoller (DLCZ)-protocol. These authors suggested to use atomic ensembles as quantum memories and linear optics combined with single-photon detection for entanglement distribution, swapping, and (built-in) distillation. This proposal influenced experiments and theoretical investigations and led to improved protocols based on atomic ensembles and linear optics (see [30] for a recent review).

To our knowledge, the most efficient scheme based on atomic ensembles and linear optics was proposed very recently by Minář *et al* [21]. These authors suggest to use heralded qubit amplifiers [53] to produce entanglement on demand and then to extend it using entanglement swapping based on two-photon detections. The state produced at the end of the protocol no longer contains vacuum components and therefore can be used directly for QKD. This is an improvement over the original DLCZ protocol in



**Figure 12.** Hybrid quantum repeater with imperfect quantum operations ( $p_G = 0.995$ ) and imperfect detectors ( $\eta_d = 0.9$ ): Optimal secret key rate (26) for the BB84-protocol as a function of the total distance  $L$ , for various numbers of segments  $2^N$  and rounds of distillation  $k$ . For  $N = 5$ , it is not possible to obtain a secret key when distillation is applied.

which the final long-distance pair is still contaminated by a fairly large vacuum term that accumulates during the imperfect storage and swapping processes<sup>‡</sup>

In this section, we first review the protocol proposed in [21] and then we analyse the role of the parameters and the performance in relation to QKD.

### 5.1. The set-up

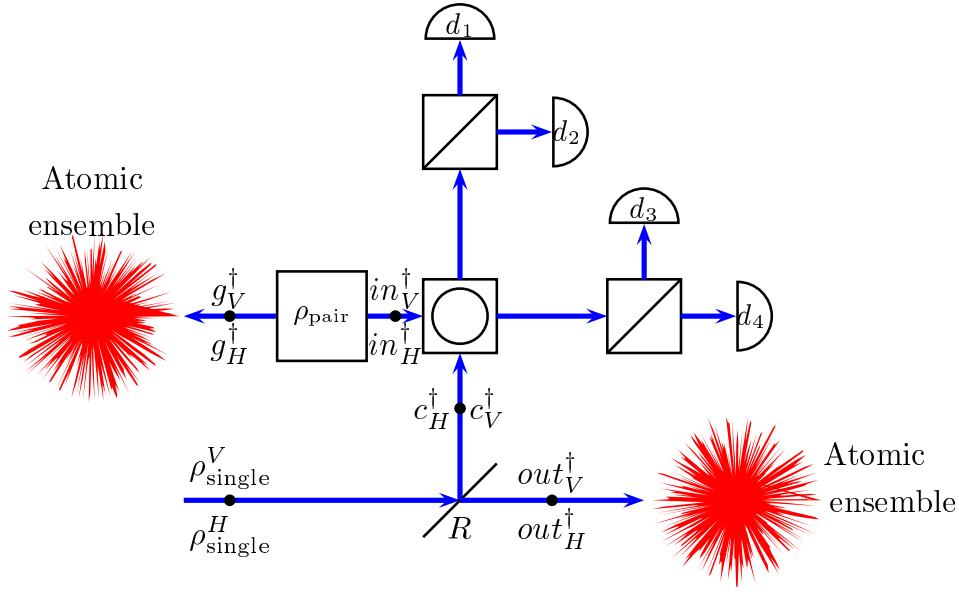
The protocol is organized in three logical steps. First, local entanglement is created in a repeater station, then it is distributed, and finally it is extended over the entire distance[21].

As a probabilistic entangled-pair source we consider spontaneous parametric down-conversion (SPDC) which produces the state [56, 57]<sup>§</sup>

$$\rho_{\text{pair}} := (1 - p) \sum_{m=0}^{\infty} \frac{2^m p^m}{(m!)^2 (m+1)} (B^\dagger)^m |0\rangle \langle 0| B^m, \quad (27)$$

<sup>‡</sup> Very recently it was shown that in the context of QKD over continuous variables, an effective suppression of channel losses and imperfections can also be achieved via a virtual, heralded amplification on the level of the classical post-processing [54, 55]. In this case, it is not even necessary to physically realize a heralded amplifier.

<sup>§</sup> In our calculation, similar to [21], we consider only those terms with  $m \leq 2$ . The reason is that the contribution to the total trace of the first three terms is given by  $1 - p^3$  and therefore for  $p < 0.1$  the state obtained by considering only the first three terms differs in a negligible way from the full state.



**Figure 13.** Quantum repeater based on atomic ensembles: Set-up for creation of on-demand entanglement (see also [21]). The whole set-up is situated at one physical location. A pair source produces the state  $\rho_{\text{pair}}$ . One part of the pair (the mode  $g$ ) is stored in an atomic ensemble and the other part (mode  $in$ ) goes into a linear-optics network. A single-photon source produces the states  $\rho_{\text{single}}^H$  and  $\rho_{\text{single}}^V$  which go through a beam splitter of reflectivity  $R$ . The output modes of the beam splitter are called  $c$  and  $out$ . The mode  $out$  is stored in a quantum memory and the mode  $c$  goes into a linear-optics network which is composed of a polarizing beam splitter in the diagonal basis  $\pm 45^\circ$  (square with a circle inside), two polarizing beam splitters in the rectilinear basis (square with a diagonal line inside), and four detectors.

where  $B^\dagger := (g_H^\dagger in_H^\dagger + g_V^\dagger in_V^\dagger)/\sqrt{2}$ . The operator  $g_i^\dagger$  ( $in_i^\dagger$ ) denotes a spatial mode with polarization given by  $i = H, V$ . The *pump parameter*  $p$  is related to the probability to have an  $n$ -photon pulse by  $P(n) = p^n(1 - p)$ .

A probabilistic single-photon source with efficiency  $q$  produces states of the form

$$\rho_{\text{single}}^i := (1 - q) |0\rangle \langle 0| + q a_i^\dagger |0\rangle \langle 0| a_i, \quad (28)$$

where  $a_i^\dagger$  ( $a_i$ ) is the creation (annihilation) operator of a photon with polarization  $i = H, V$ .

We also define by  $\gamma_{\text{rep}}$  the smallest repetition rate among the repetition rates of the SPDC source and the single-photon sources.

*On-demand entanglement source* The protocol that produces local entangled pairs works as follows (see figure 13 and [21] for additional details):

- (i) The state  $\rho_{\text{pair}} \otimes \rho_{\text{single}}^H \otimes \rho_{\text{single}}^V$  is produced.
- (ii) The single photons, which are in the same spatial mode, are sent through a tunable beam splitter of reflectivity  $R$  corresponding to the transformation  $a_i \rightarrow \sqrt{R} c_i + \sqrt{1 - R} out_i$ .

- (iii) The spatial modes *in* and *c* are sent through a linear-optics network which is part of the heralded qubit amplifiers, and the following transformations are realized,

$$c_H \rightarrow \frac{d_3 + d_4 + d_2 - d_1}{2}, \quad c_V \rightarrow \frac{d_3 + d_4 - d_2 + d_1}{2}, \quad (29)$$

$$in_H \rightarrow \frac{d_2 + d_1 + d_3 - d_4}{2}, \quad in_V \rightarrow \frac{d_2 + d_1 - d_3 + d_4}{2}, \quad (30)$$

where  $d_1, d_2, d_3, d_4$  are four spatial modes, corresponding to the four detectors.

- (iv) A twofold coincidence detection between  $d_1$  and  $d_3$  (or  $d_1$  and  $d_4$  or  $d_2$  and  $d_3$  or  $d_2$  and  $d_4$ ) projects the modes *g* and *out* onto an entangled state. These are the heralding events that acknowledge the storage of an entangled pair in the quantum memories *out* and *g*. The probability of a successful measurement is given by

$$P_0^s(p, q, R, \eta_d) = 4 \text{tr} \left( \Pi_{d_1}^1(\eta_d) \Pi_{d_2}^0(\eta_d) \Pi_{d_3}^1(\eta_d) \Pi_{d_4}^0(\eta_d) \rho'_{g, out, d_1, d_2, d_3, d_4} \right), \quad (31)$$

where  $\rho'_{g, out, d_1, d_2, d_3, d_4}$  is the total state obtained at the end of step (iii) and the superscript *s* stands for source. The POVM for the detectors has been defined in (2). The factor 4 accounts for the fact that there are four possible twofold coincidences. The resulting state is

$$\rho_0^s(p, q, R, \eta_d) = \frac{4}{P_0^s} \text{tr}_{d_1, d_2, d_3, d_4} \left( \Pi_{d_1}^1(\eta_d) \Pi_{d_2}^0(\eta_d) \Pi_{d_3}^1(\eta_d) \Pi_{d_4}^0(\eta_d) \rho'_{g, out, d_1, d_2, d_3, d_4} \right). \quad (32)$$

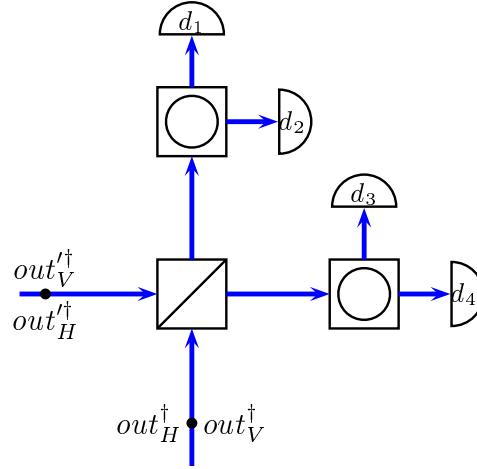
This is the locally prepared state that will be distributed between the repeater stations.

In the ideal case with perfect detectors and perfect single-photon sources, the resulting state (after a suitable rotation) is  $\rho_0^s = |\phi^+\rangle \langle \phi^+|$  which can be obtained with probability  $P_0^s = pR(1 - R)$ . In the realistic case, however, additional higher-order excitations are present. In [21], the explicit form of  $\rho_0^s$  and  $P_0^s$  can be found for the case when  $1 > R \gg p$  and  $1 \gg 1 - q$ .

Therefore, we have seen that the protocol proposed in [21] permits to turn a probabilistic entangled-pair source (SPDC in our case) into an on-demand entangled photon source. In this context *on-demand* means that when a heralding event is obtained then it is known for sure that an entangled quantum state is stored in the quantum memories *out* and *g*.

*Entanglement distribution and swapping* Once local entangled states are created, it is necessary to distribute the entanglement over segments of length  $L_0$  and then to perform entanglement swapping. Both procedures are achieved in a similar way (see figure 14), as we shall describe in this section. Entanglement distribution is done as follows (see figure 14 and [21] for additional details):

- (i) Each of the two adjacent stations create a state of the form  $\rho_0^s$ . We call *g* and *out* the modes belonging to the first station and *g'* and *out'* the modes of the second station.



**Figure 14.** Quantum repeater based on atomic ensembles: Set-up used for entanglement distribution (swapping) (see [21] for additional details). The modes  $out$  and  $out'$  are released from two quantum memories separated by distance  $L_0$  (or located at the same station for the case of swapping) and sent into a linear-optics network consisting of one polarizing beam splitter in the rectilinear basis (square with diagonal line inside), two polarizing beam splitters in the diagonal basis (square with circle inside), and four detectors.

- (ii) The modes  $out$  and  $out'$  are read out from the quantum memories and sent through an optical fibre to a central station where a linear-optics network is used in order to perform entanglement swapping. The transformations of the modes are as follows:

$$\begin{aligned} out_H &\rightarrow \frac{d_3 + d_4}{\sqrt{2}}, & out_V &\rightarrow \frac{d_1 - d_2}{\sqrt{2}}, \\ out'_H &\rightarrow \frac{d_1 + d_2}{\sqrt{2}}, & out'_V &\rightarrow \frac{d_3 - d_4}{\sqrt{2}}, \end{aligned}$$

where  $d_1, d_2, d_3, d_4$  are four spatial modes.

- (iii) A twofold coincidence detection between  $d_1$  and  $d_3$  (or  $d_1$  and  $d_4$  or  $d_2$  and  $d_3$  or  $d_2$  and  $d_4$ ) projects the modes  $out$  and  $out'$  onto an entangled state. The probability of this event is given by

$$P_0(p, q, R, \eta_d, \eta_{mtd}) = 4 \operatorname{tr} \left( \Pi_{d_1}^1(\eta_{mtd}) \Pi_{d_2}^0(\eta_{mtd}) \Pi_{d_3}^1(\eta_{mtd}) \Pi_{d_4}^0(\eta_{mtd}) \rho'_{g,g',d_1,d_2,d_3,d_4} \right), \quad (33)$$

where  $\rho'_{g,g',d_1,d_2,d_3,d_4}$  is the total state obtained at the end of step (ii) and  $\eta_{mtd} := \eta_m \eta_t \left( \frac{L_0}{2} \right) \eta_d$ , with  $\eta_m$  being the probability that the quantum memory releases a photon. The factor 4 accounts for the fact that there are four possible twofold coincidences. The resulting state is

$$\rho_{0,g,g'} = \frac{4}{P_0} \operatorname{tr}_{d_1,d_2,d_3,d_4} \left( \Pi_{d_1}^1(\eta_{mtd}) \Pi_{d_2}^0(\eta_{mtd}) \Pi_{d_3}^1(\eta_{mtd}) \Pi_{d_4}^0(\eta_{mtd}) \rho'_{g,g',d_1,d_2,d_3,d_4} \right). \quad (34)$$

The state  $\rho_{0,g,g'}$  is the entangled state shared between two adjacent stations over distance  $L_0$ . In order to perform entanglement swapping, the same steps as described above are repeated until those two stations separated by distance  $L$  are finally connected.

Formally, the probability that entanglement swapping is successful in the nesting level  $n$  is given by

$$P_{ES}^{(n)}(p, q, R, \eta_d, \eta_{\text{mtd}}) = 4 \operatorname{tr} \left( \Pi_{d_1}^1(\eta_{md}) \Pi_{d_2}^0(\eta_{md}) \Pi_{d_3}^1(\eta_{md}) \Pi_{d_4}^0(\eta_{md}) \rho'_{n-1, g, g', d_1, d_2, d_3, d_4} \right), \quad (35)$$

where  $\rho'_{n-1, g, g', d_1, d_2, d_3, d_4}$  is the total state resulting from steps (i) and (ii) described above in this section, and  $\eta_{md} := \eta_m \eta_d$ . The swapped state is given by

$$\rho_{n, g, g'} = \frac{4}{P_{ES}^{(n)}} \operatorname{tr}_{d_1, d_2, d_3, d_4} \left( \Pi_{d_1}^1(\eta_{md}) \Pi_{d_2}^0(\eta_{md}) \Pi_{d_3}^1(\eta_{md}) \Pi_{d_4}^0(\eta_{md}) \rho'_{n-1, g, g', d_1, d_2, d_3, d_4} \right). \quad (36)$$

The state  $\rho_{n, g, g'}$  is the state that will be used for quantum key distribution when  $n = N$ . In a regime where higher-order excitations can be neglected, the state  $\rho_{n, g, g'}$  is a maximally entangled Bell state. In [21] it is given the expression of the state  $\rho_{n, g, g'}$  under the same assumptions on the reflectivity  $R$  and the efficiency  $q$  of the single-photon sources as discussed regarding  $\rho_0^s$  in (32).

Given the final state  $\rho_{AB} := \rho_{N, g, g'}$  it is possible to calculate  $P_{\text{click}}$  and the QBER, using the formalism of section 2.2.2 and inserting  $\eta_{md}$  for the detector efficiency.

The final secret key rate then reads

$$R_{\text{QKD}}^{\text{AE}} = R_{\text{REP}}(L_0, p, N, \eta_d, \eta_m, \gamma_{\text{rep}}, q) P_{\text{click}}(L_0, p, N, \eta_d, \eta_m, q) R_{\text{sift}} r_{\infty}^{\text{BB84}}(L_0, p, N, \eta_d, \eta_m, q), \quad (37)$$

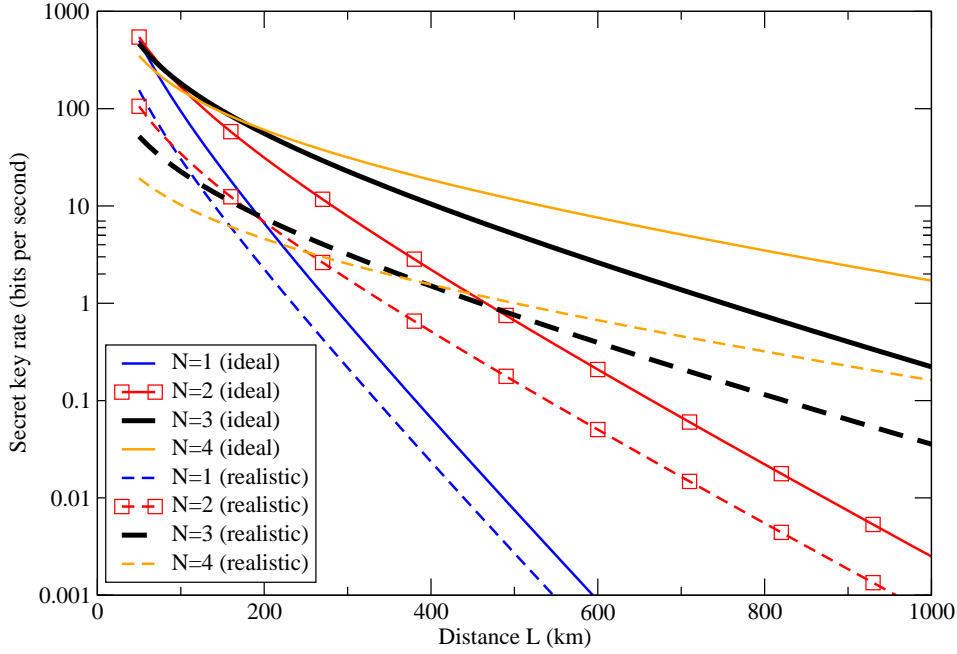
where  $R_{\text{REP}}$  is given by (8) with  $\beta = 1$  for the communication time (see figure 2c). As for the QKD protocol, we consider the asymmetric BB84-protocol ( $R_{\text{sift}} = 1$ , see section 2.2). The superscript AE stands for atomic ensembles.

## 5.2. Performance in the presence of imperfections

As in the previous sections, we shall focus on the secret key rate. The free parameters are the pump parameter  $p$  and the reflectivity of the beam splitter  $R$ . In all plots, we optimize these parameters in such a way that the secret key rate is maximized. As all optimizations have been done numerically, our results may not correspond to the global maximum, but only to a local maximum. In general, we observed that if we treat the secret key rate as a function of  $p$  (calculated at the optimal  $R$ ), the maximum of the secret key rate is rather narrow. On the other hand, when calculated as a function of  $R$  (at the optimal  $p$ ), this maximum is quite broad.

The most favourable scenario (ideal case) is characterized by perfect detectors ( $\eta_d = 1$ ), perfect quantum memories ( $\eta_m = 1$ ), and deterministic single-photon sources ( $q = 1$ ) which can emit photons at an arbitrarily high rate ( $\gamma_{\text{rep}} = \infty$ ). In this case, the heralded qubit amplifier is assumed to be able to create perfect Bell states and the secret fraction therefore becomes one. The only contribution to the secret key rate is then given by the repeater rate. In figure 15 the optimal secret key rate versus the distance, obtained by maximizing over  $p$  and  $R$ , is shown (see solid lines).

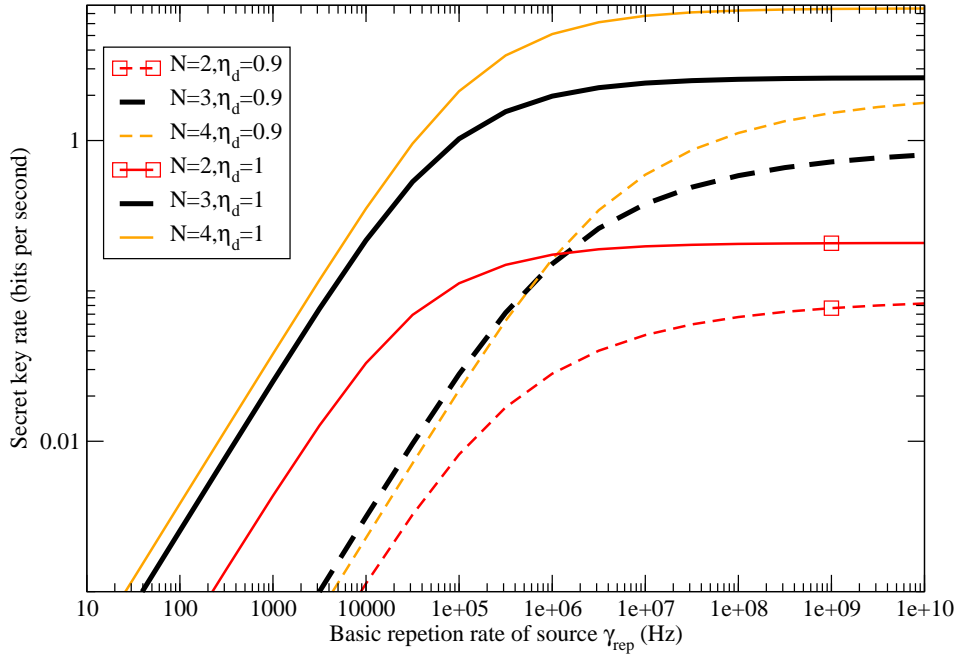
For the calculation of figure 15, we have assumed that the creation of local entanglement, i.e., of state  $\rho_0^s$ , is so fast that we can neglect the creation time. In the case of SPDC, the repetition rate of the source is related to the pump parameter  $p$  and, moreover, the single-photon sources also have finite generation rates that should



**Figure 15.** Quantum repeaters based on atomic ensembles: Optimal secret key rate per second versus the distance between Alice and Bob. The secret key rate has been obtained by maximizing over  $p$  and  $R$ . Ideal set-up (solid line) with parameters  $\eta_m = \eta_d = q = 1, \gamma_{rep} = \infty$ . More realistic set-up (dashed line) with parameters  $\eta_m = 1, \eta_d = 0.9, q = 0.96, \gamma_{rep} = 50$  MHz.

be taken into account. For this purpose, we introduce the photon-pair preparation time which is given by  $T_0^s = \frac{1}{\gamma_{rep} P_0^s}$  [21]. The formula for the repeater rate in this case corresponds to (8) with  $T_0 \rightarrow T_0 + T_0^s$ . As shown in figure 16, when  $\eta_d = 1$  the secret key rate is constant for  $\gamma_{rep} > 10^7$ , however, for realistic detectors with  $\eta_d = 0.9$ , much higher repetition rates are required in order to reach the asymptotic value. Nowadays, SPDC sources reach a rate of about 100 MHz, whereas single-photon sources have a repetition rate of a few MHz [47]. Recently, a new single-photon source with repetition rate of 50 MHz has been realized [58]. In the following, we will employ  $\gamma_{rep} = 50$  MHz.

A consequence of imperfect detectors is that multi-photon pulses contribute to the final state. The protocol we are considering here is less robust against detector inefficiencies than the original DLCZ protocol. This is due to the fact that successful entanglement swapping is conditioned on twofold detection as compared to one-photon detection of the DLCZ protocol. However, twofold detections permit to eliminate the vacuum in the memories [30], thus increasing the final secret key rate. As shown in figure 17, the secret key rate spans four orders of magnitude as  $\eta_d$  increases from 0.7 to 1. Thus, an improvement of the detector efficiency causes a considerable increase of the secret key rate. For example, for  $N = 3$ , an improvement from  $\eta_d = 0.85$  to  $\eta_d = 0.88$  leads to a threefold increase of the secret key rate. Notice that we have considered photon detectors which are able to resolve photon numbers. Photon detectors with an efficiency as high as 95% have been realized [59]. These detectors work at the telecom



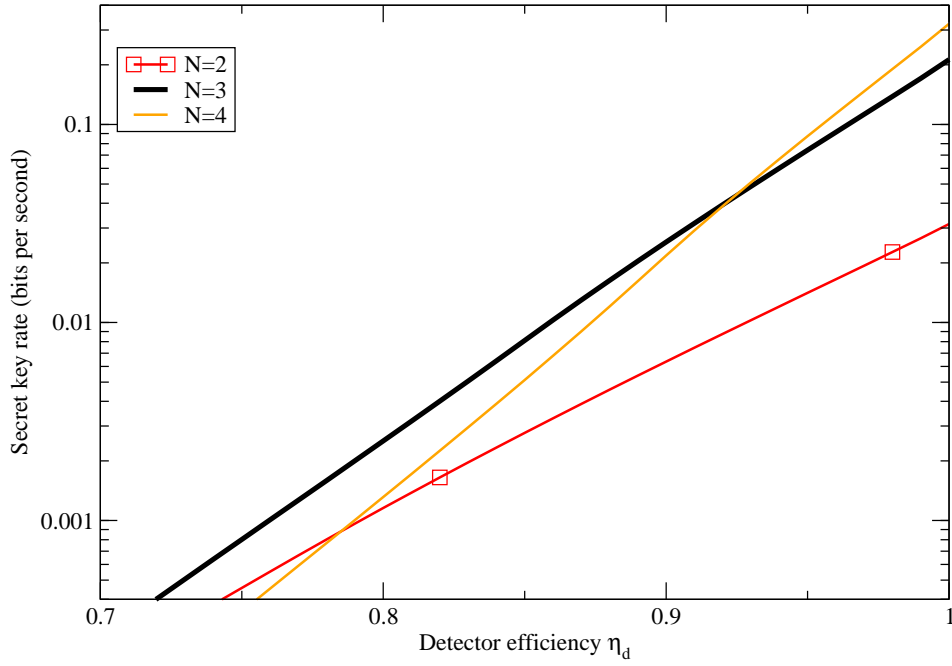
**Figure 16.** Quantum repeaters based on atomic ensembles: Optimal secret key rate per second versus the basic repetition rate of the source  $\gamma_{\text{rep}}$ . The secret key rate has been obtained by maximizing over  $p$  and  $R$ . (Parameters:  $\eta_d = \eta_m = q = 1$ ).

bandwidth of 1556 nm and they have negligible dark counts. The drawback is that they need to operate at very low temperatures of 100 mK. The reading efficiency of the quantum memory  $\eta_m$  plays a similar role as the detector efficiency. In accordance to [30], intrinsic quantum memory efficiencies above 80% have been realized [60]; however, total efficiencies where coupling losses are included are much lower.

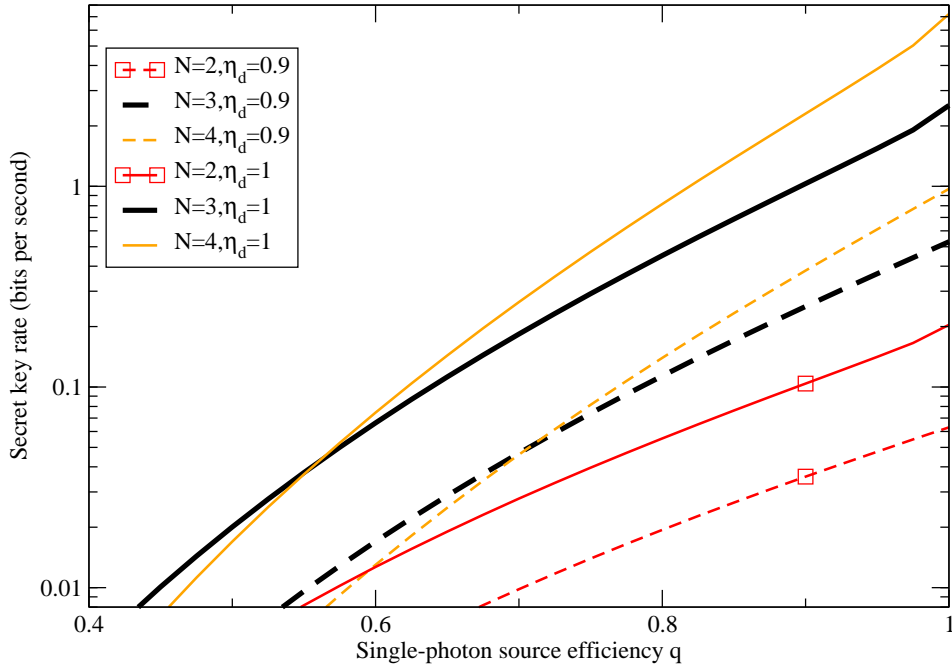
A single-photon source is also characterized by its efficiency, i.e., the probability  $q$  to emit a photon. As shown in figure 18, we see that it is necessary to have single-photon sources with high efficiencies, in particular, when detectors are imperfect. The source proposed in [58] reaches  $q = 0.96$ .

In figure 15 we show the secret key rate as a function of the distance between Alice and Bob for parameters (dashed lines) which are optimistic in the sense that they could be possibly reached in the near future. We observe that with an imperfect set-up and for  $N = 4$ , the realistic secret key rate is by one order of magnitude smaller than the ideal value. This decrease is mainly due to finite detector efficiencies. For  $N = 4$ , the secret key rate scales proportionally to  $\eta_d^2 \eta_d^2 \eta_d^{2 \cdot 4} \eta_d^2$  (local creation, distribution, entanglement swapping, and QKD measurement). For  $\eta_d = 0.9$ , finite detector efficiencies lead to a decrease of the secret key rate by 78%. Regarding the optimal pump parameter  $p$ , we observe in figure 19 that for large distances ( $L > 600\text{km}$ ) its value is about 0.15%. The order of magnitude of this value is in agreement with the results found in [20] regarding the original DLCZ protocol and the BB84-protocol. The optimal reflectivity  $R$  is given in figure 20. We observe that as  $N$  increases, the optimal value of  $R$  has a modest increase.

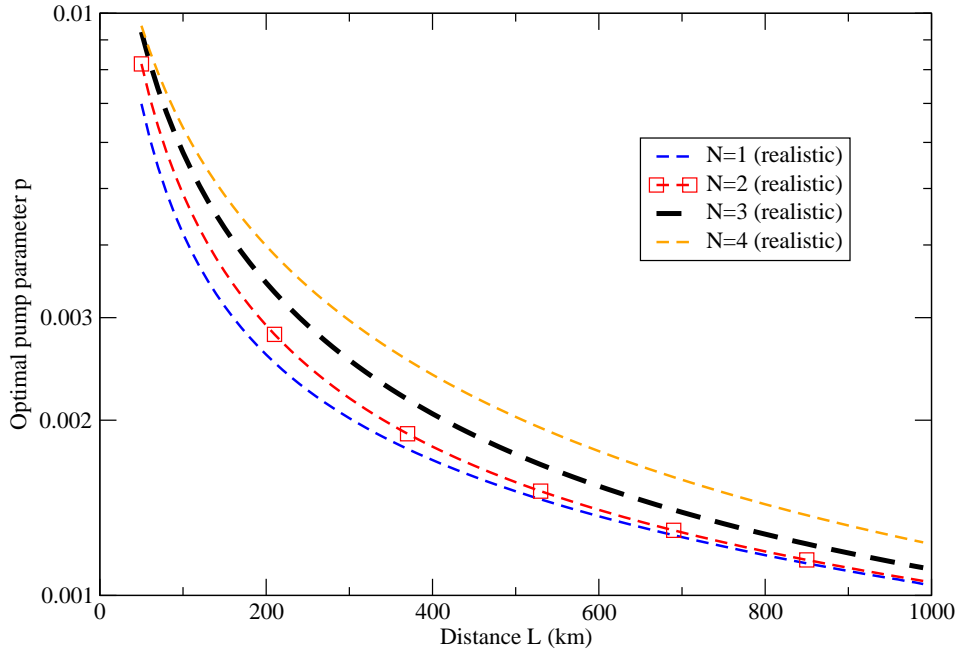




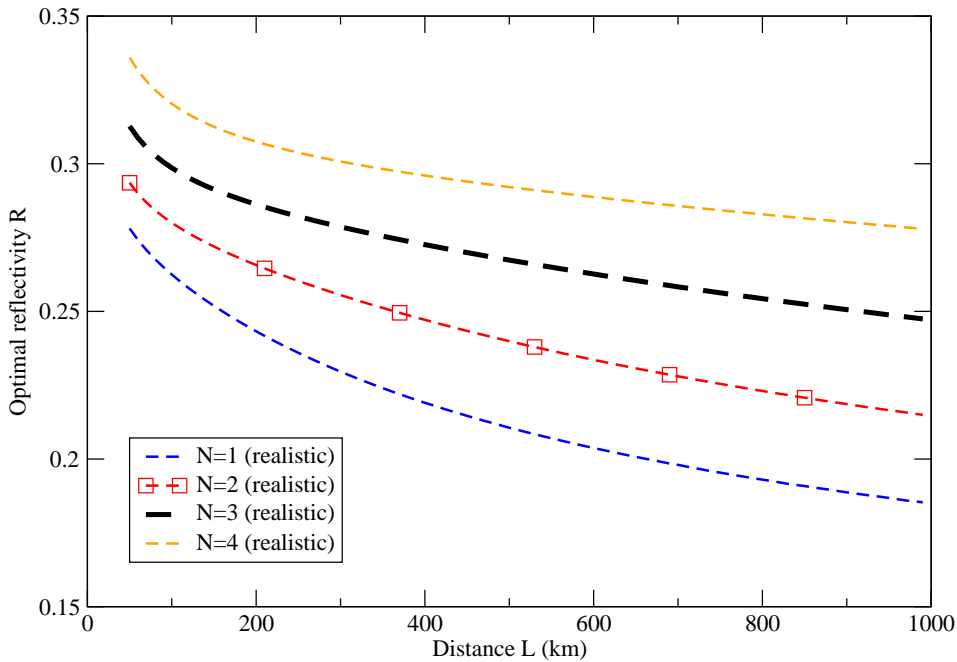
**Figure 17.** Quantum repeaters based on atomic ensembles: Optimal secret key rate per second versus the efficiency of the detectors  $\eta_d$ . The secret key rate has been obtained by maximizing over  $p$  and  $R$ . (Parameters:  $\eta_m = q = 1$ ,  $\gamma_{\text{rep}} = 50$  MHz).



**Figure 18.** Quantum repeaters based on atomic ensembles: Optimal secret key rate per second versus the probability to emit a single photon. The secret key rate has been obtained by maximizing over  $p$  and  $R$ . (Parameters:  $\eta_m = 1$ ,  $\gamma_{\text{rep}} = 50$  MHz).



**Figure 19.** Quantum repeaters based on atomic ensembles: Optimal value of  $p$  versus the distance between Alice and Bob. The corresponding secret key rate is shown in figure 15. (Parameters:  $\eta_m = 1$ ,  $\eta_D = 0.9$ ,  $q = 0.96$ ,  $\gamma_{rep} = 50$  MHz)



**Figure 20.** Quantum repeaters based on atomic ensembles: Optimal value of the reflectivity  $R$  versus the distance between Alice and Bob. The corresponding secret key rate is shown in figure 15. (Parameters:  $\eta_m = 1$ ,  $\eta_D = 0.9$ ,  $q = 0.96$ ,  $\gamma_{rep} = 50$  MHz)

## 6. Conclusions

Quantum repeaters represent nowadays the most promising and advanced approach to create long-distance entanglement. Quantum key distribution (QKD) is a developed

technology which has already reached the market. One of the main limitations of current QKD is that the two parties have a maximal separation of 150 km, due to losses in optical fibres. In this paper, we have studied long-distance QKD by using quantum repeaters.

We have studied three of the main protocols for quantum repeaters, namely, the original protocol, the hybrid quantum repeater, and a variation of the so-called DLCZ protocol. Our analysis differs from previous treatments, in which only final fidelities have been investigated, because we have maximized the main figure of merit for QKD – the secret key rate. Such an optimization is non-trivial, since there is a trade-off between the repeater pair-generation rate and the secret fraction: the former typically decreases when the final fidelity grows, whereas the latter would increase when the final fidelity becomes larger.

Since it is hard to compare different protocols directly, as there are different experimental requirements and difficulties for each of them, here we investigated the main aspects for every protocol separately.

The general type of quantum repeater is a kind of prototype for a quantum repeater based on the original proposal [7]. We have provided an estimate of the experimental parameters needed to extract a secret key and showed what the role of each parameter is. We have found that the requirement on the initial fidelity is not so strong if distillation is allowed (even for  $F_0 = 0.9$ , it is possible to have one secret bit per second). However, quantum gates need to be very good (errors of the order of 1%).

Further, we have studied the hybrid quantum repeater. This protocol permits to perform both the initial entanglement distribution and the entanglement swapping with high efficiencies. The reason is that bright light sources are used for communication and Cavity Quantum Electrodynamics (CQED) interactions are employed for the local quantum gates, making the swapping, in principle, deterministic. We have found that finite detector efficiencies do not play a major role with regards to the generation probability. This permits to have high secret key rates in a set-up where it is possible to neglect imperfections of the detectors. By studying imperfect gates we found that excellent gates are necessary (errors of the order of 0.1%).

Finally, we have considered repeaters with atomic ensembles and linear optics. There exist many experimental proposals and therefore we have studied the scheme which is believed to be the fastest [21]. This scheme uses heralded qubit amplifiers for creating dual-rail encoded entanglement and entanglement swapping based on two-fold detection events. In contrast to the previous two schemes, the Bell measurement used for entanglement swapping is not able to distinguish all four Bell states. We have characterized all common imperfections and we have seen that using present technology, the performance of this type of quantum repeater in terms of secret key rates is only about one order of magnitude different from the corresponding ideal set-up. Thus, this scheme seems robust against most imperfections. These types of repeater schemes, as currently being restricted to linear optics, could still be potentially improved by allowing for additional nonlinear-optics elements. This may render the entanglement swapping steps deterministic, similar to the hybrid quantum repeater using CQED, and thus

further enhance the secret key rates.

For all those protocols considered here, single-qubit rotations were assumed to be perfect. Obviously, this assumption is not correct in any realistic situation. However, most of these single-qubit rotations can be replaced by simple bit flips of the classical outcomes which are used when the QKD protocol starts. Therefore, we see that in this case, specifically building a quantum repeater for QKD applications permits to relax the requirements on certain operations that otherwise must be satisfied for a more general quantum application, such as distributed quantum computation.

In conclusion, quantum repeaters could be a possible solution for long-distance QKD. However, in order to achieve performances comparable to current short-distance QKD systems, it will be necessary to operate in parallel many of those set-ups considered in this paper, possibly including additional multiplexing strategies.

## Acknowledgments

The authors acknowledge financial support by the German Federal Ministry of Education and Research (BMBF, project QuOREP). The authors would like to thank the organizers and participants of the quantum repeater workshops (project QuOREP) held in Hannover and Bad Honnef in 2011 and 2012. N. K.B. and P. v.L. thank the Emmy Noether Program of the Deutsche Forschungsgemeinschaft for financial support. S. A. thanks J. Minář for enlightening discussions and insightful comments.

## Appendix A. Additional material for the general framework

### *Appendix A.1. Generation rate with probabilistic entanglement swapping and distillation*

In this appendix, we give the derivation of (8) in section 2.1.2 which describes the generation rate of entangled pairs per time unit  $T_0$  with probabilistic entanglement swapping and distillation, i.e.,

$$R_{\text{REP}}^{\text{prob}} := \frac{1}{T_0} \left(\frac{2}{3}\right)^{N+k} P_0 P_{ES}^{(1)} P_{ES}^{(2)} \dots P_{ES}^{(N)} \prod_{i=1}^k P_D[i]. \quad (\text{A.1})$$

In [30] the formula has been derived only for the case without distillation and there it reads as follows,

$$R_{\text{REP}}^{\text{prob}} := \frac{1}{T_0} \left(\frac{2}{3}\right)^N P_0 P_{ES}^{(1)} P_{ES}^{(2)} \dots P_{ES}^{(N)}, \quad (\text{A.2})$$

where  $P_0$  is the probability to generate a pair for entanglement swapping. This formula was derived for small  $P_0$ .

In order to incorporate distillation into (A.2) we use the definition of the recursive probability  $P_{L_0}[k]$  given in (6), see [33]. It describes the generation probability of an

entangled pair after  $k$  rounds of purification. If we use that  $Z_1(x) = \frac{3-2x}{x(2-x)} \leq \frac{3}{2x}$  for small  $x$ , we can rewrite  $P_{L_0}[k]$ :

$$\begin{aligned} P_{L_0}[k] &= \frac{P_D[k]}{Z_1(P_{L_0}[k-1])} \leq \frac{2}{3} P_D[k] P_{L_0}[k-1] \\ &= \frac{2}{3} P_D[k] \frac{P_D[k-1]}{Z_1(P_{L_0}[k-2])} \leq \dots \leq \left(\frac{2}{3}\right)^k P_0 \prod_{i=1}^k P_D[i], \end{aligned} \quad (\text{A.3})$$

where we used in the last line that  $P_{L_0}[k]$  is a recursive formula. For deriving (A.1), we replace in (A.2)  $P_0$  by  $P_{L_0}$  and we use (A.3).

## Appendix B. Additional material for the original quantum repeater

### Appendix B.1. Entanglement swapping

*The protocol* We consider the total state  $\rho_{ab} \otimes \rho_{cd}$ . The entanglement swapping algorithm consists of the following steps:

- (i) A CNOT is applied on system  $b$  as source and  $c$  as target.
- (ii) One output system is measured in the computational basis and the other one in the basis  $\{|+\rangle := \frac{|H\rangle+|V\rangle}{\sqrt{2}}, |-\rangle = \frac{|H\rangle-|V\rangle}{\sqrt{2}}\}$ , obtained by applying a Hadamard gate.
- (iii) In the standard entanglement swapping algorithm, a single qubit rotation depending on the outcome of the measurement is performed. However, for the purpose of QKD it is not necessary to do this single-qubit rotation\*. We propose that Bob collects the results of the Bell measurements, performs the standard QKD measurement and then he can apply a classical bit flip depending on the QKD measurement basis and on the Bell measurement outcomes.

*Formulas in the presence of imperfections* We consider a set-up with two detectors  $d_1$  and  $d_2$ . We associate the detection pattern of these two detectors with a two-dimensional Hilbert space, e.g.  $d_1 = \text{click}, d_2 = \text{noclick} \Rightarrow |H\rangle = |1_{d_1}, 0_{d_2}\rangle$  and  $d_1 = \text{noclick}, d_2 = \text{click} \Rightarrow |V\rangle = |0_{d_1}, 1_{d_2}\rangle$  where  $\{|H\rangle, |V\rangle\}$  are a basis of a two-dimensional Hilbert space which can be, for example, identified with horizontal and vertical polarizations of a qubit. We discard those events where there are no clicks or when both detectors click. If the detectors are imperfect, we may have an error in the detection of the quantum state. The POVM consists of two elements  $\Pi_H$  ( $\Pi_V$ ) which detect mode  $|H\rangle$  ( $|V\rangle$ ):

$$\Pi_H := \gamma |H\rangle \langle H| + (1 - \gamma) |V\rangle \langle V|, \quad (\text{B.1})$$

$$\Pi_V := \gamma |V\rangle \langle V| + (1 - \gamma) |H\rangle \langle H|, \quad (\text{B.2})$$

with

$$\gamma := \frac{\eta_d + p_{\text{dark}}(1 - \eta_d)}{\eta_d + 2p_{\text{dark}}(1 - \eta_d)}, \quad (\text{B.3})$$

\* Note that this step is different from [7], where the single-qubit rotations were explicitly included.

where  $p_{\text{dark}}$  is the dark count probability of the detectors and  $\eta_d$  is their efficiency<sup>†</sup>.

The POVM above has been used also in [7, 61], however, the connection with the imperfections of the detectors was not made.

If we start with the states  $\rho_{ab} = \rho_{cd} = A|\phi^+\rangle\langle\phi^+| + B|\phi^-\rangle\langle\phi^-| + C|\psi^+\rangle\langle\psi^+| + D|\psi^-\rangle\langle\psi^-|$ , the resulting state after entanglement swapping between  $a$  and  $d$  is still a Bell diagonal state with coefficients of the form:

$$\begin{aligned} A' &= \frac{1-p_G}{4} + p_G [\gamma^2(A^2 + B^2 + C^2 + D^2) + 2(1-\gamma^2)(AD + BC) \\ &\quad + 2\gamma(1-\gamma)(A+D)(C+B)], \\ B' &= \frac{1-p_G}{4} + p_G [2\gamma^2(AB + CD) + 2(1-\gamma^2)(AC + BD) \\ &\quad + \gamma(1-\gamma)(A^2 + B^2 + C^2 + D^2 + 2AD + 2BC)], \\ C' &= \frac{1-p_G}{4} + p_G [2\gamma^2(AC + BD) + 2(1-\gamma^2)(AB + CD) \\ &\quad + \gamma(1-\gamma)(A^2 + B^2 + C^2 + D^2 + 2AD + 2BC)], \\ D' &= \frac{1-p_G}{4} + p_G [2\gamma^2(AD + BC) + (1-\gamma^2)(A^2 + B^2 + C^2 + D^2) \\ &\quad + 2\gamma(1-\gamma)(A+D)(B+C)], \end{aligned} \tag{B.4}$$

and the probability to obtain the state above is equal to

$$P_{ES}(\eta, p_{\text{dark}}) := ((1-p_{\text{dark}})(\eta_d + 2p_{\text{dark}}(1-\eta_d)))^2, \tag{B.5}$$

which can be interpreted as the probability that entanglement swapping is successful<sup>‡</sup>. Note that  $P(\eta, 0) = \eta^2$  and  $P(1, 0) = 1$  as we expect. When we consider dark counts  $p_{\text{dark}} < 10^{-5}$ , then these are negligible as  $(P_{ES}(0.1, 10^{-5})/(P_{ES}(0.1, 0)))^N < 1.03^N$ , so the impact on the secret key rate is minimal.

## Appendix B.2. Distillation

*The protocol* We assume that Alice and Bob hold two Bell diagonal states  $\rho_{a_1, b_1}$  and  $\rho_{a_2, b_2}$ . The algorithm is the following:

<sup>†</sup> The coefficient  $\gamma$  can be calculated as follows: the POVM for having a click under the assumption of single-photon sources and imperfect detectors is given by

$$E^{(\text{click})} = p_{\text{dark}}|0\rangle\langle 0| + (1 - (1 - p_{\text{dark}})(1 - \eta_d))|1\rangle\langle 1|$$

and no click

$$E^{(\text{noclick})} = (1 - p_{\text{dark}})|0\rangle\langle 0| + (1 - p_{\text{dark}})(1 - \eta_d)|1\rangle\langle 1|.$$

When we say that the detector  $a$  clicked, and  $b$  did not click and we discard the vacuum events, and those where both detectors clicked, the POVM looks as follows:

$$\begin{aligned} E_a^{(\text{click})} \otimes E_b^{(\text{noclick})} &= (1 - (1 - p_{\text{dark}})(1 - \eta_d))(1 - p_{\text{dark}})|1_a, 0_b\rangle\langle 1_a, 0_b| \\ &\quad + p_{\text{dark}}(1 - p_{\text{dark}})(1 - \eta_d)|0_a, 1_b\rangle\langle 0_a, 1_b|. \end{aligned}$$

The trace is  $(1 - p_{\text{dark}})(\eta_d + 2p_{\text{dark}}(1 - \eta_d))$ , which is exactly the probability that we have this measurement. If we normalize this measurement and relate it to the POVM in (B.1), we get  $\gamma$ .

<sup>‡</sup> This probability was derived by taking the probability of the measurement in the preceding footnote squared, as we need two coincident clicks for the Bell measurement.

- (i) In the computational basis, Alice rotates her particles by  $\frac{\pi}{2}$  about the  $X$ -axis, whereas Bob applies the inverse rotation ( $-\frac{\pi}{2}$ ) on his particles.
- (ii) Then they apply on both sides a CNOT operation, where the states  $a_1$  ( $b_1$ ) serve as source and  $a_2$  ( $b_2$ ) as target.
- (iii) The states corresponding to the target are measured in the computational basis. If the measurement results coincide, the resulting state  $\rho_{a_1, b_1}$  is a purified state; otherwise, the resulting state is discarded. Therefore, this entanglement distillation scheme is probabilistic.

*Formulas in the presence of imperfections* Given a Bell diagonal state with the following coefficients

$$\rho_{ab} = A |\phi^+\rangle \langle \phi^+| + B |\phi^-\rangle \langle \phi^-| + C |\psi^+\rangle \langle \psi^+| + D |\psi^-\rangle \langle \psi^-|, \quad (\text{B.6})$$

the coefficients transform according to the following map [27]:

$$A' = \frac{1}{P_D} (A^2 + D^2), \quad (\text{B.7})$$

$$B' = \frac{1}{P_D} (2AD), \quad (\text{B.8})$$

$$C' = \frac{1}{P_D} (B^2 + C^2), \quad (\text{B.9})$$

$$D' = \frac{1}{P_D} (2BC), \quad (\text{B.10})$$

where  $P_D$  is the probability that the measurement outcomes are both the same for Alice and Bob, and thus the probability of successful distillation is:

$$P_D[k] = (A_{k-1} + D_{k-1})^2 + (B_{k-1} + C_{k-1})^2. \quad (\text{B.11})$$

Including the gate quality  $p_G$ , these formulas change to [62]:

$$P_D[k] = \frac{1}{2} \{1 + p_G^2 (-1 + 2A_{k-1} + 2D_{k-1})^2\}. \quad (\text{B.12})$$

with

$$\begin{aligned} A' &= [1 + p_G^2 ((A - B - C + D)(3A + B + C + 3D) + 4(A - D)^2)] / (8P_D), \\ B' &= [1 - p_G^2 (A^2 + 2A(B + C - 7D) + (B + C + D)^2)] / (8P_D), \\ C' &= [1 + p_G^2 (4(B - C)^2 - (A - B - C + D)(A + 3(B + C) + D))] / (8P_D), \\ D' &= [1 - p_G^2 (A^2 + 2A(B + C + D) + B^2 + 2B(D - 7C) + (C + D)^2)] / (8P_D). \end{aligned}$$

## Appendix C. Additional material for the hybrid quantum repeater

### Appendix C.1. Entanglement generation

The total state before the detector measurements is described by [50]

$$\rho_{AB, b_3, b_5} = p \left( (|0\rangle_{b_3} |00\rangle_{AB} |\beta\rangle_{b_5} + |11\rangle_{AB} |-\beta\rangle_{b_5}) / 2 \right)$$

$$\begin{aligned}
& + |0\rangle_{b_5} (|01\rangle_{AB} |-\beta\rangle_{b_3} + |10\rangle_{AB} |\beta\rangle_{b_3})/2)) \times H.c.) + \\
(1-p) & ((|0\rangle_{b_3} (|00\rangle_{AB} |\beta\rangle_{b_5} - |11\rangle_{AB} |-\beta\rangle_{b_5})/2 \\
& + |0\rangle_{b_5} (|01\rangle_{AB} |-\beta\rangle_{b_3} - |10\rangle_{AB} |\beta\rangle_{b_3})/2)) \times H.c.), \tag{C.1}
\end{aligned}$$

where *H.c.* stays for the Hermitian conjugate of the previous term,  $A$  ( $B$ ) represents the qubit at Alice's (Bob's) side,  $b_3$  is the coherent-state mode arriving at the detector  $D_1$ ,  $b_5$  is the coherent-state mode arriving at the detector  $D_2$ , and  $\beta = i\sqrt{2\eta_t} \sin(\theta/2)$  (see figure (8)). The probability of error caused by photon losses in the transmission channel is given by  $(1-p)$ , with  $p = (1 + e^{-2(1-\eta_t)\alpha^2 \sin^2(\theta/2)})/2$ . It is possible to observe from (C.1) that whenever Bob detects a click in either one of the detectors  $D_1$  or  $D_2$ , an entangled state has been distributed between qubits  $A$  and  $B$ .

We discuss in the following the case that  $D_1$  and  $D_2$  are imperfect PNRD (see (2)). When detector  $D_1$  does not click and  $D_2$  clicks, the resulting state  $\rho_{AB}$  is then given by

$$\rho_{AB} = \frac{\text{tr}_{b_3 b_5} (\Pi_{b_3}^{(0)} \Pi_{b_5}^{(n)} \rho_{AB, b_3, b_5})}{\text{tr} (\Pi_{b_3}^{(0)} \Pi_{b_5}^{(n)} \rho_{AB, b_3, b_5})}, \tag{C.2}$$

with  $n > 0$ . The same result up to local operations can be obtained in the opposite case (a click in detector  $D_1$  and no click in detector  $D_2$ ).

Depending on the outcome of the detector, a local operation maybe applied to change the resulting state into the desired state. In this way, if the outcome is an even number, nothing should be done, otherwise a  $Z$  operation should be applied. Following this, the resulting state can be written as

$$\rho = F_0 |\phi^+\rangle \langle \phi^+| + (1 - F_0) |\phi^-\rangle \langle \phi^-|, \tag{C.3}$$

where

$$\begin{aligned}
F_0 &= \frac{(\langle 00|_{AB} + (-1)^n \langle 11|_{AB})}{\sqrt{2}} \rho_{A,B} \frac{(|00\rangle_{AB} + (-1)^n |11\rangle_{AB})}{\sqrt{2}} \\
&= \frac{1 + e^{-2(1+\eta_t(1-2\eta_d))\alpha^2 \sin^2(\theta/2)}}{2}. \tag{C.4}
\end{aligned}$$

The probability of success is calculated by adding all successful events, and is given by

$$P_0 = \sum_{n=1}^{\infty} \text{tr} (\Pi_{b_3}^{(0)} \Pi_{b_5}^{(n)} \rho_{AB, b_3, b_5} + \Pi_{b_5}^{(0)} \Pi_{b_3}^{(n)} \rho_{AB, b_3, b_5}), \tag{C.5}$$

after some transformation this can be written as in (23).

### Appendix C.2. Entanglement swapping

The initial states used in the swapping operation are a full rank mixture of the Bell states,  $\rho_0 := A |\phi^+\rangle \langle \phi^+| + B |\phi^-\rangle \langle \phi^-| + C |\psi^+\rangle \langle \psi^+| + D |\psi^-\rangle \langle \psi^-|$ . After the connection, the resulting state will remain in the same form,  $A' |\phi^+\rangle \langle \phi^+| + B' |\phi^-\rangle \langle \phi^-| + C' |\psi^+\rangle \langle \psi^+| + D' |\psi^-\rangle \langle \psi^-|$ , but with new coefficients:

$$\begin{aligned}
A' &= 2BC + 2AD + 2(-2BC + A(B + C - 2D) + (B + C)D)p_G \\
&\quad + (A - B - C + D)^2 p_G^2,
\end{aligned}$$



$$\begin{aligned}
B' &= 2AC + 2BD + (A^2 + (B + C)^2 - 4BD + D^2 + 2A(-2C + D))p_G \\
&\quad - (A - B - C + D)^2 p_G^2, \\
C' &= 2AB + 2CD + (A^2 + (B + C)^2 - 4CD + D^2 + 2A(-2B + D))p_G \\
&\quad - (A - B - C + D)^2 p_G^2, \\
D' &= A^2 + B^2 + C^2 + D^2 - 2(A^2 + B^2 + C^2 - A(B + C) - (B + C)D + D^2)p_G \\
&\quad + (A - B - C + D)^2 p_G^2.
\end{aligned} \tag{C.6}$$

It is possible to see that  $A' + B' + C' + D' = 1$ , such that even for the case of imperfect connection operations, the swapping occurs deterministically.

### Appendix C.3. Entanglement distillation

We calculated also the effect of the gate error in the distillation step. Starting with two copies of states in the form of  $\rho_0 := A |\phi^+\rangle \langle \phi^+| + B |\phi^-\rangle \langle \phi^-| + C |\psi^+\rangle \langle \psi^+| + D |\psi^-\rangle \langle \psi^-|$ , the resulting state after one round of distillation is given by  $A' |\phi^+\rangle \langle \phi^+| + B' |\phi^-\rangle \langle \phi^-| + C' |\psi^+\rangle \langle \psi^+| + D' |\psi^-\rangle \langle \psi^-|$ , where

$$\begin{aligned}
A' &= \frac{1}{P_D} \left( D^2 + A^2(1 + 2(-1 + p_G)p_G)^2 - 2A(-1 + p_G)p_G(C + 2D + 2(B - C - 2D)p_G \right. \\
&\quad \left. + 2(-B + C + 2D)p_G^2) - 2D(-1 + p_G)p_G(-2D - 2(C + D)(-1 + p_G)p_G \right. \\
&\quad \left. + B(1 + 2(-1 + p_G)p_G)) \right), \\
B' &= \frac{1}{P_D} \left( -2(D(-1 + p_G)p_G(C + D + 2Bp_G - 2Cp_G - 2Dp_G - 2Bp_G^2 + 2Cp_G^2 + 2Dp_G^2) \right. \\
&\quad \left. + A^2p_G(-1 + 3p_G - 4p_G^2 + 2p_G^3) - A(D(1 - 2p_G + 2p_G^2)^2 \right. \\
&\quad \left. - (-1 + p_G)p_G(-2C(-1 + p_G)p_G + B(1 - 2p_G + 2p_G^2))) \right), \\
C' &= \frac{1}{P_D} \left( B^2(1 - 2p_G + 2p_G^2)^2 - 2B(-1 + p_G)p_G(-2A(-1 + p_G)p_G + D(1 - 2p_G + 2p_G^2) \right. \\
&\quad \left. + C(2 - 4p_G + 4p_G^2)) + C(C(1 - 2p_G + 2p_G^2)^2 \right. \\
&\quad \left. - 2(-1 + p_G)p_G(-2D(-1 + p_G)p_G + A(1 - 2p_G + 2p_G^2))) \right), \\
D' &= \frac{1}{P_D} \left( -2(C(-1 + p_G)p_G(C + D + 2Ap_G - 2Cp_G - 2Dp_G - 2Ap_G^2 + 2Cp_G^2 + 2Dp_G^2) \right. \\
&\quad \left. + B^2p_G(-1 + 3p_G - 4p_G^2 + 2p_G^3) - B(C(1 - 2p_G + 2p_G^2)^2 \right. \\
&\quad \left. - (-1 + p_G)p_G(-2D(-1 + p_G)p_G + A(1 - 2p_G + 2p_G^2))) \right), \tag{C.7}
\end{aligned}$$

$P_D$  is the distillation probability of success and is given by

$$P_D = (B + C)^2 + (A + D)^2 - 2(A - B - C + D)^2 p_G + 2(A - B - C + D)^2 p_G^2. \tag{C.8}$$

For the case of  $p_G = 1$ , (C.7) and (C.8) are in accordance with [27].

## References

- [1] Ekert A 1991 *Phys. Rev. Lett.* **67** 661
- [2] Pitkanen D, Ma X, Wickert R, van Loock P and Lütkenhaus N 2011 *Phys. Rev. A* **84** 022325
- [3] Curty M and Moroder T 2011 *Phys. Rev. A* **84** 010304

- [4] Gisin N, Pironio S and Sangouard N 2010 *Phys. Rev. Lett.* **105** 070501
- [5] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
- [6] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
- [7] Briegel H J, Dür W, Cirac J I and Zoller P 1998 *Phys. Rev. Lett.* **81** 5932
- [8] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
- [9] Collins D, Gisin N and De Riedmatten H 2005 *J. Mod. Optic.* **52** 735
- [10] de Riedmatten H, Marcikic I, Tittel W, Zbinden H, Collins D and Gisin N 2004 *Phys. Rev. Lett.* **92** 047904
- [11] Waks E, Zeevi A and Yamamoto Y 2002 *Phys. Rev. A* **65** 052310
- [12] Duan L M, Lukin M D, Cirac J I and Zoller P 2001 *Nature* **414** 413
- [13] van Loock P, Ladd T D, Sanaka K, Yamaguchi F, Nemoto K, Munro W J and Yamamoto Y 2006 *Phys. Rev. Lett.* **96** 240501
- [14] Sangouard N, Dubessy R and Simon C 2009 *Phys. Rev. A* **79** 042340
- [15] Zhao B, Müller M, Hammerer K and Zoller P 2010 *Phys. Rev. A* **81** 052329
- [16] Han Y, He B, Heshami K, Li C Z and Simon C 2010 *Phys. Rev. A* **81** 052311
- [17] Childress L, Taylor J M, Sørensen A S and Lukin M D 2005 *Phys. Rev. A* **72** 052330
- [18] Scherer A, Sanders B C and Tittel W 2011 *Opt. Express* **19** 3004
- [19] Razavi M, Amirloo J and Majedi A 2010 Quantum key distribution over atomic-ensemble quantum repeaters *Optical Fiber Communication (OFC), collocated National Fiber Optic Engineers Conference, 2010 Conference on (OFC/NFOEC)* pp 1–3
- [20] Amirloo J, Razavi M and Majedi A H 2010 *Phys. Rev. A* **82** 032304
- [21] Minář J, de Riedmatten H and Sangouard N 2012 *Phys. Rev. A* **85** 032313
- [22] Bratzik S, Abruzzo S, Kampermann H and Bruß D *In preparation*
- [23] Tatarskiĭ V 1961 *Wave propagation in a turbulent medium* (New York: McGraw-Hill)
- [24] Kok P and Lovett B W 2010 *Introduction to optical quantum information processing* (Cambridge: Cambridge University Press)
- [25] Hartmann L, Kraus B, Briegel H and Dür W 2007 *Phys. Rev. A* **75** 032310
- [26] Razavi M, Piani M and Lütkenhaus N 2009 *Phys. Rev. A* **80** 032301
- [27] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
- [28] Żukowski M, Zeilinger A, Horne M and Ekert A 1993 *Phys. Rev. Lett.* **71** 4287
- [29] Pan J W, Bouwmeester D, Weinfurter H and Zeilinger A 1998 *Phys. Rev. Lett.* **80** 3891
- [30] Sangouard N, Simon C, de Riedmatten H and Gisin N 2011 *Rev. Mod. Phys.* **83** 33
- [31] Cabrillo C, Cirac J I, García-Fernández P and Zoller P 1999 *Phys. Rev. A* **59** 1025
- [32] Feng X L, Zhang Z M, Li X D, Gong S Q and Xu Z Z 2003 *Phys. Rev. Lett.* **90** 217902
- [33] Bernardes N K, Praxmeyer L and van Loock P 2011 *Phys. Rev. A* **83** 012323
- [34] Renner R 2008 *Int. J. Quantum Inf.* **6** 1
- [35] Bennett C H and Brassard G 1984 Quantum cryptography: Public key distribution and coin tossing *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* vol 175 (Bangalore, India)
- [36] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
- [37] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018
- [38] Bechmann-Pasquinucci H and Gisin N 1999 *Phys. Rev. A* **59** 4238
- [39] Beaudry N J, Moroder T and Lütkenhaus N 2008 *Phys. Rev. Lett.* **101** 093601
- [40] Renner R, Gisin N and Kraus B 2005 *Phys. Rev. A* **72** 012332
- [41] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 080501
- [42] Renner R and König R 2005 Universally composable privacy amplification against quantum adversaries *Theory of Cryptography Conference (TCC)* vol 3378 (Springer) p 407
- [43] Müller-Quade J and Renner R 2009 *New J. Phys.* **11** 085006
- [44] Lo H K, Chau H and Ardehali M 2005 *J. Cryptol.* **18** 133

- [45] Wolfram Research I 2010 *Mathematica Edition: Version 8.0* (Wolfram Research, Inc.)
- [46] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 *Phys. Rev. A* **54** 3824
- [47] Eisaman M, Fan J, Migdall A and Polyakov S 2011 *Rev. Sci. Instrum* **82** 071101
- [48] Ladd T D, van Loock P, Nemoto K, Munro W J and Yamamoto Y 2006 *New J. Phys.* **8** 184
- [49] van Loock P, Lütkenhaus N, Munro W J and Nemoto K 2008 *Phys. Rev. A* **78** 062319
- [50] Azuma K, Sota N, Namiki R, Özdemir Ş, Yamamoto T, Koashi M and Imoto N 2009 *Phys. Rev. A* **80** 060303
- [51] van Loock P, Munro W J, Nemoto K, Spiller T P, Ladd T D, Braunstein S L and Milburn G J 2008 *Phys. Rev. A* **78** 022303
- [52] Louis S G R, Munro W J, Spiller T P and Nemoto K 2008 *Phys. Rev. A* **78** 022326
- [53] Ralph T and Lund A 2009 Nondeterministic noiseless linear amplification of quantum systems *AIP Conference Proceedings* vol 1110 p 155
- [54] Fiurasek J and Cerf N J 2012 *ArXiv e-prints (Preprint 1205.6933)*
- [55] Walk N, Symul T, Lam P K and Ralph T C 2012 *ArXiv e-prints (Preprint 1206.0936)*
- [56] Kwiat P G, Mattle K, Weinfurter H, Zeilinger A, Sergienko A V and Shih Y 1995 *Phys. Rev. Lett.* **4337**
- [57] Kok P and Braunstein S L 2000 *Phys. Rev. A* **61** 042304
- [58] Lee K, Chen X, Eghlidi H, Kukura P, Lettow R, Renn A, Sandoghdar V and Göttinger S 2011 *Nature Photon.* **5** 166
- [59] Lita A, Miller A and Nam S 2008 *Opt. express* **16** 3032
- [60] Simon C, de Riedmatten H, Afzelius M, Sangouard N, Zbinden H and Gisin N 2007 *Phys. Rev. Lett.* **98** 190503
- [61] Dür W, Briegel H J, Cirac J I and Zoller P 1999 *Phys. Rev. A* **59** 169–181
- [62] Dür W 1998 *Quantum communication over long distances using quantum repeaters* Diplomarbeit Leopold-Franzens-Universität Innsbruck Innsbruck